MOVING BEYOND CONSENT IN DATA PRIVACY LAW

AN EFFECTIVE PRIVACY MANAGEMENT SYSTEM FOR INTERNET SERVICES

By

MARCIN BETKIER

A thesis
submitted to the Victoria University of Wellington
in fulfilment of the requirements for the degree of
Doctor of Philosophy

Victoria University of Wellington
2018

"As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread, permanently connecting him to the local centre of personnel records administration. There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. The point is that a so-called completely clean record was almost unattainable, an ideal, like absolute truth. Something negative or suspicious can always be noted down against any man alive. Everyone is guilty of something or has something to conceal. All one has to do is to look hard enough to find out what it is.

Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads who manage personnel records administration, that most complicated science, and for these people's authority."

Aleksandr Solzhenitsyn, *Cancer Ward*

Abstract

This thesis looks for a way to overcome the failure of consent as a means of addressing privacy problems associated with online services. It argues that consent to collection and use of personal data is an imperfect mechanism for individual authorisation because data privacy in relation to online services is a dynamic, continuous process. If people are to have autonomous choice in respect of their privacy processes, then they need to be able to manage these processes themselves.

After careful examination of online services which pinpoints both the privacy problems caused by online service providers and the particular features of the online environment, the thesis devises a set of measures to enable individuals to manage these processes. The tool for achieving this is a Privacy Management Model (PMM) which consists of three interlocking functions: controlling (which consent may be a part of), organising, and planning.

The thesis then proposes a way of implementing these functions in the context of online services. This requires a mix of regulatory tools: a particular business model in which individuals are supported by third parties (Personal Information Administrators), a set of technical/architectural tools to manage data within the ICT systems of the online service providers, and laws capable of supporting all these elements.

The proposed legal measures aim to overcome the shortcomings of procedural principles by implementing a comprehensive model in which substantive legal principle underpins a bundle of statutory-level laws which enable privacy management functions. Those are explained against the background of the General Data Protection Regulation. All of this is designed to change the way decision-makers think about Internet privacy and form the theoretical backbone of the next generation of privacy laws.

Acknowledgements

First and foremost I would like to express my deepest gratitude to Nicole Moreham for her supervision, being generous with time, knowledge, and practical advice, and for her thoughtfulness. I received also a lot of helpful advice and guidance from Tony Angelo for which I am immensely thankful. Furthermore, I would like to thank my secondary supervisor, Susy Frankel for her insightful and constructive comments, which helped me to avoid many reefs in the course of my studies. Also, I will not forget about invaluable comments and suggestions from Graeme Austin, Petra Butler, Carwyn Jones, Katarzyna Szymielewicz, Katrine Evans, David De Joux, Antonio Pabón Cadavid, and Nikita Melashchenko which I received on different stages of my journey.

I appreciated very much the professional and thoughtful help from Jonathan Dempsey and professional staff of the Law Faculty. Also, I am grateful to Victoria University for a Doctoral Scholarship which allowed me to work with peace of mind during these years.

I saved an enormous amount of time thanks to Frank Bennett and the excellent Juris-M resource manager which helped me to organise my research base and automated my work on citations. Also, I am grateful for the final proofreading of a professional editor Madeleine Collinge, who provided her services in accordance with the Editorial Advice Policy of Victoria University of Wellington.

Dear fellow PhD students, thank you for the friendship, help, advice I received, and writing sessions in the railway station bar.

Last, but not least, my wife, Ewa, and my children Basia and Witek have given me a tremendous amount of love and support over these years. I could have done nothing without this.

Foreword

A couple of years ago, I worked as a regulatory expert for a large corporation. I remember the meeting I had with my colleague who was working in the unit specialising in technological innovations. I loved that part of my job, as it was related to discussing fresh, innovative, and often brilliant ideas. That particular meeting was about privacy requirements for the user interface of one of the future mobile apps. The project was in a preliminary phase, the stress level was low, and we were having a friendly chat together with a third colleague from the unit responsible for data protection in a conference room surrounded by glass walls fading out the hustle and bustle of the big firm.

In the conversation, I briefly described the legal role of customer consent and we were informally discussing when the provision in the Terms & Conditions of the service was necessary and when the app should additionally prompt its users for consent. The conclusion was that collecting consent was the most difficult response for all of the questions resulting from the app's use-case scenarios. And then, I said the sentence which changed my life: "Well, it looks like privacy is not a kidney, you can sell it for the benefits from the service." I remember that my other colleague from the data protection unit threw me a rather strange, withering look, but she said nothing. However, this made me think about that sentence. And, after some time this thinking and talking to privacy experts pushed me into a journey to the other side of the globe and into a three-year study, at the end of which, I have to say, I am far from being proud of what I said.

The questions I had on my mind were: What exactly is privacy and why do we protect our data? Is privacy more like a commodity, which can be sold, or more like part of the body, eliminated from trade? What sort of 'magic' works by the means of a data subject's consent that it is the response to many of the questions about the legality of data activities? Should consent have such an important role? How is it placed in other jurisdictions? And, how does it happen that, despite having free choice, as a result, individuals may be more deprived of their privacy than they probably would be without such choice? Is there any better way to make sure that individual interests in privacy are protected, and, at the same time, online services can develop?

This thesis contains all the responses.

Table of Contents

List of Abbreviations

API	Application Programming Interface;
Article 29 WP	Article 29 Working Party – an advisory body of representatives from the DPAs of each EU Member State;
BVerfG	*Bundesverfassungsgericht* – German Federal Constitutional Tribunal;
ChFREU	Charter of Fundamental Rights of the European Union;
CJEU	Court of Justice of the European Union;
Convention 108	Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108;
DNT	'Do Not Track' (technology standard);
DPA	Data Protection Authority;
DPD	Data Protection Directive – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995;
ECHR	European Convention on Human Rights – The Convention for the Protection of Human Rights and Fundamental Freedoms;
ECtHR	European Court of Human Rights;
ePrivacy Directive	Directive on privacy and electronic communications – Directive 2002/58/EC of the European Parliament and of the Council of 12 July October 1995;
FIPPs	Fair Information Practice Principles;
GDPR	General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
ICT	Information and Communications Technology;
OECD	Organisation for Economic Co-operation and Development;
OECD Guidelines	Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development (1981, amended in 2013);
P3P	Platform for Privacy Preferences (technology standard);
PDS	Personal Data Store;
PIA	Personal Information Administrator;
PIMS	Personal Information Management System;

PIPEDA	Personal Information Protection and Electronic Documents Act 2000 (Canada);
PMM	Privacy Management Model;
T&Cs	Terms and Conditions;
UI	User Interface;
VRM	Vendor Relationship Management.

I Introduction

An information technology revolution is transforming many aspects of society and the economy. To cite the phrase coined by Google: "We no longer go online, we live online." This shift is underpinned by the processing of personal data. Those data come from many sources: websites, mobile apps, sensors, networks, and cameras. They describe real people – data subjects. Personal data can create a detailed picture of who they are, what they have been doing, with whom, what they have seen or told, and what they are looking for. Such digital profiles may be compared with the profiles of others to make inferences about data subjects. The creation of such profiles is the main goal of many online service providers since they can be monetised by selling the information about data subjects piece by piece to those who are interested in influencing them. This mechanism is universal and can serve anybody who wants data subjects to buy a product or be convinced of an idea. The result is that Internet users are not only stalked with advertisements; messages are also tailored to their particular personal traits which exposes them to a range of risks. This not only influences their consumer behaviour but shapes their social interactions and affects societies as a whole – it can even tip the balance of the elections. The better the profile of these individuals, the more vulnerable they are to discrimination, manipulation, coercion, or 'identity theft'. This affects their autonomy and dignity and has serious social consequences; free, liberal democracy cannot exist without free, autonomous individuals. Paradoxically, data subjects not only consent to this mechanism of corporate surveillance, they pay for it, usually in the price of the end products. All this suggests that consent mechanisms fail to express autonomous choice with respect to data privacy.

The main contribution of this thesis is a proposed solution to this failure of consent or, more broadly, to the problem of a lack of suitable tools enabling individuals to exercise their informational autonomy online. This is a significant problem experienced by almost every person using the Internet: all they have is the 'all or nothing' choice between benefiting from modern digital technology and keeping their personal data away from the extensive corporate surveillance. The thesis provides a theoretical framework and a set of conceptual tools to reject this dichotomy and put individuals in the driver's seat. It also devises a set of regulatory tools which can remedy the structural problems of the Internet which arise from the architectural

and informational imbalances. The proposed solution is effective in the sense that it enables the effective exercise of individual autonomy and, at the same time, facilitates the effective operation of online services. This latter point recognises that the use of personal data is necessary for the modern economy. To that end, the thesis analyses economic and technical details of online services and plans out regulation by means of a particular set of economic, architectural, and legal tools.

Four aspects of this proposal are particularly novel. First, the thesis redefines the privacy interest in personal data as management of a privacy process. This broadened view provides a new perspective in the legal sciences and enables one to realise why consent fails. It shifts the focus away from securing the single procedural action of giving consent to implementing a comprehensive tool which facilitates autonomous choice in the individual privacy process.

Second, the thesis presents a theoretical model to manage privacy processes – the Privacy Management Model (PMM). The three functions at the core of PMM – organising, planning, and controlling – describe the elements necessary for data subjects to have autonomous choice in respect of their privacy processes. Although there have been some limited references to the idea of managing consent or privacy in the literature, privacy management has not, to the author's knowledge, previously been identified as a regulatory instrument nor broken down into its constituent functions.

Third, the thesis develops a completely new privacy-aware business model based on trusted third parties, Personal Information Administrators (PIAs). There have been many ideas to introduce third parties to counterbalance the power of online service providers, but moving data management functions to a separate data flow and employing PIAs to help individuals in managing their data is novel. The idea is that individual privacy policies held by PIAs would have precedence over the default privacy settings of service providers. PIAs may then act as users' proxies to monitor their data use and respond to authorisation requests. This removes from both individuals and service providers the burden of serving and reading the deluge of consent requests and enables individuals to use technology on their own terms. Giving individuals agency over their personal data also helps to build trust between them and service providers. Furthermore, it avoids paternalism and makes it possible to accommodate the whole

panoply of different perceptions of privacy within unified global services. So, in other words, the idea is a potential win-win solution.

Fourth, proposed privacy laws overcome the shortcomings of the widespread model of procedural privacy principles. The thesis provides a comprehensive framework of statutory-level laws underpinned by a legal freedom, which together can form the theoretical backbone of the next generation of privacy laws. Applying the proposed laws precisely to the privacy-infringing activities may also allow regulators to reduce the burden which data protection laws place on other personal data users, who do not engage in those activities. In the author's opinion this would be a much welcomed change.

A Guide to the Thesis

The thesis comprises two Parts. Part I describes the failure of consent while Part II presents the solution to this failure, namely effective implementation of privacy management. The first Part describes (in Chapter II) the nature of the privacy interest in respect of personal data processing and the role of consent. First, it briefly presents online trends. It explains necessary terms, the importance of personal data, and the particular characteristics of online data processing. This is also the place to describe the particular group of data controllers on which the thesis focuses – online service providers. Second, it defines data privacy as informational self-determination (autonomy) and puts this in the context of theoretical discussions about privacy. This is to show that the nature of privacy can be explained as a mix of, on the one hand, tangible values which can be described in the language of economics, and, on the other hand, intangible, personal values protecting inalienable values, like dignity, autonomy, and participation in a society. This gives some authors reason to treat personal data as a constitutive part of someone's identity and individuality. (So, data may actually resemble a part of the human body much more closely than the author had predicted in the anecdote in Foreword.) But, privacy is also a dynamic, social process in which individuals reveal some information about themselves in a controlled way. Third, the thesis uses this insight about data privacy to show the role of consent as a procedural method of autonomous authorisation. It explains why consent fails in respect of a privacy process and that the autonomous authorisation of data processing may be achieved by means of a different, more complete tool – privacy management. Privacy management is, therefore, described as the capacity of data subjects to

govern the process of collection and use of their data with the ability to control data and their use, monitor the process, and plan. These operations also require the process to be organised in a particular way.

Chapter III describes the challenges posed by Internet services. This description serves as a 'threat model' which provides a framework for working out a solution. First, it shows how 'data markets' work, what are the key success factors in online businesses and how this influences their models. Such business models are described by reference to their impact on the informational autonomy of data subjects. This allows the thesis to pinpoint data activities (like online tracking, profiling, and using data brokers) and a particular business model (non-trading platform) which infringe privacy. It also shows how the economic value of personal data is created, how it can be conceptualised and measured, and that such value is derived from its personal value. Second, this chapter examines the characteristics of the online environment focussing on actors and their relationships. This shows that the fact that the relevant actions take place in the (usually centralised) ICT architecture of online service providers causes an imbalance of power and a surge of corporate surveillance which heavily limits individuals' choices. This is a systemic problem which causes online customers to be perfectly described ('individualised') and exposed to the actions of data users. The chapter then points to the adverse consequences of those activities – privacy problems. It explains how and when the risk of tangible loss is created and increased, how this risk eventuates, how harm to dignity and autonomy results, and what interference with social values this can lead to. All the above not only shows what is wrong with some online services, but also makes key points for a policy discussion in the next chapter. This concludes Part I.

Once all the symptoms of the "privacy illness" have been described, Part II draws the plan of action. This plan, consistently with the title of the thesis, leads to the construction of an effective privacy management system. This effectiveness, as explains Chapter IV, has two faces: the effective protection of privacy values and the effective operation of 'data markets'. Both these aspects of effectiveness have to be demonstrated. To that end, firstly, this chapter briefly discusses the problems of privacy regulations and defines the main regulatory tool: Privacy Management Model (PMM). This is a theoretical mechanism to control privacy processes by the means of its three main functions: organising, planning, and controlling (in which consent may play a part). Those functions are explained and the relevant test for

evaluating them is presented. This test is used thereafter as a set of operational goals to design and verify privacy regulations. Secondly, this chapter shows why regulating privacy by means of PMM could be beneficial for both data subjects and service providers. The PMM model can be an additional mechanism applied to those online services which pose the problems identified in Part I. Relieving individuals and service providers from the burden of consent requirements without leaving individuals vulnerable to privacy breaches has a huge potential. Individuals would get better control over their privacy processes, whilst trustworthy online service providers would get less risky and more flexible access to some data. Thirdly, the chapter examines the toolbox of available regulatory techniques. It recognises that PMM could be implemented by a mix of market (economic regulations), technology (architecture/code), and law. Furthermore, it recognises that the best place to implement PMM is the European Union as it exports higher privacy standards to other jurisdictions.

Having set out the model that should be implemented (ie PMM), Chapter V considers economic regulations. That is to say, it asks whether market forces work effectively and how they could be steered towards greater respect for informational autonomy. First, it discusses the state of market competition (as privacy can be understood as an aspect of service quality) and shows why the 'invisible hand of the market' and self-regulation (norms) do not work and bad privacy practices dominate in the market. Second, the chapter presents the 'business model' for implementing PMM – a set of measures to influence the market. The most important of them is the use of third parties called Personal Information Administrators (PIAs), who could support individuals in exercising their informational autonomy. PIAs could provide individuals with necessary expertise and technical tools for privacy management and, at the same time, create a fiduciary relationship with them (since they would not benefit from monetising their personal data). Furthermore, they could hold the privacy policies of individuals and, as well as monitoring privacy processes, act as proxies for individuals in responding to possible authorisation (consent) requests. This should be complemented by other measures for influencing markets and supporting individuals, such as data portability, increasing their 'data sensitivity', and securing them from uncontrolled tracking.

Chapter VI explains how to implement privacy management and the PIA business model in technology regulation. It discusses two specific areas: technologies used to express and communicate privacy decisions and technologies supporting enforcement and accountability.

There are examples of failures of industry self-regulation (norms) in those areas, but, it concludes, the technical means for privacy management are largely available. Privacy policy languages and the means to build the necessary interfaces are available; but, they need to be improved to cover the PIA business model and developed into a formal technical description of functionality to execute the PMM functions. Furthermore, Chapter VI sets out what an 'ontology' of data and data uses would look like and explains how it could be used to present data subjects with a simple set of options. Finally, this chapter analyses mechanisms for enforcement and accountability concluding that, despite a dearth of current off-the-shelf solutions, a framework enabling enforcement of privacy management and accountability of practice (verifying actual data practices) could be delivered. To achieve such accountability, any technology mechanism needs to be supported by robust privacy laws.

The laws implementing PMM, described in Chapter VII, should be shaped slightly differently from current data privacy laws. Firstly, this chapter identifies the gaps in the existing legislation. Those gaps are found at the base level of the framework of Fair Information Practice Principles (FIPPs) which underpins the privacy law in all researched jurisdictions and the controlling mechanisms contained therein. The chapter then describes how contemporary statutory mechanisms fit into privacy management. Secondly, the thesis shows how to close those gaps using the example of the regulations in the European General Data Protection Regulation (GDPR). It is shown in detail what functionalities the relevant legal provisions need to deliver to achieve the operational goals set out earlier in each of the key areas of PMM: controlling, organising, and planning. Thirdly, the thesis discusses the general legal requirements necessary to guarantee that the regulation is successful. These requirements relate to the extraterritorial reach of the law, the need to regulate the right actors and activities, and, most importantly, the enactment of an overarching principle in place of the FIPPs schema – the right to informational self-determination. The thesis proposes the specific formulation of this right and shows how it fits into the existing European privacy rights.

The last chapter, Chapter VIII, is a brief, high-level summary of the key elements of the regulatory mix needed to implement the Privacy Management Model into practice.

B Note about Methodology

The regulation of services mediated by technology is specific, as it combines multiple areas of knowledge: law, economics, and technology. To get to the nub of the problem with consent, it is necessary to describe all these three dimensions. However, this is primarily a legal thesis that presents as a full a picture as possible of the researched problem and necessary regulatory response. So, the ideas set out herein were developed mainly by means of critical studies of legal theories, relevant Acts, and cases. This also included secondary sources like texts, journal articles, opinions of authoritative bodies, and proposals for new legislation. They are all detailed in the Bibliography at the end of the thesis. The broadest part of the research was dedicated to the ethical and moral origins of privacy, autonomy, and consent, which took the author into aspects of medical law, bioethics, and communication theory. The legal analysis also has a historical aspect because it focuses on the origins of concepts underpinning contemporary data privacy laws.

The sole purpose of this thesis is to set out what the effective implementation of privacy management should look like. To do this, it analyses the potential accommodation of PMM in a range of jurisdictions. The jurisdictions discussed are New Zealand, Australia, Canada, and European law as it is applied in the UK. European law is understood as a sum of jurisdictions of the Council of Europe and the European Union. These jurisdictions have been chosen because they give a good overview of the different roles of consent (and individual participation) in data privacy laws but remain, at the same time, easy to compare because of a common origin and existing connections between them (membership of the Commonwealth, the OECD, and, in the case of the UK, the European Union and Council of Europe). Some very important concepts were also drawn from German jurisprudence and different United States sources. Despite the numerous jurisdictions examined, the thesis compares them only to find the best ideas for implementing the privacy management system.

The peculiarity of the field of regulation and a broad understanding of regulation itself make it necessary to analyse the business side of online services and technology. This is because consent is given in the context of the particular market behaviour of service providers and by the means of technology. Furthermore, the mix of the proposed regulatory tools consists of economic regulation and technical (architectural) measures. They are all necessary to

effectively address the subject-matter of the problem. However, technology and market-related concepts are described broadly, using the language of the problems they cause or functionalities they can (or cannot) deliver, and avoiding any formal language (ie notations defining technology or economics in a formal way). The goal of using them is not to present or create a full description of economic theory or technological frameworks but to show the nature of observed phenomena and explain the applied solutions. Such an approach can only touch on the rich debates in these areas of science but is kept within the limits of what is necessary to present this thesis.

PART I

THE FAILURE OF CONSENT

II What is Data Privacy and What is the Role of Consent?

This chapter introduces privacy with respect to data processing[1] and defines the theoretical concepts which underpin the thesis. Part A introduces necessary terms and presents factual background related to data processing activities. This presents the main actors: online service providers and data subjects, personal data, and how they are used. Knowing this enables Part B to explain what data privacy *is* and what privacy is *worth*. That is to say, it defines data privacy as informational self-determination (or autonomy) of the individual and puts it in a wider theoretical context. It also describes the nature of data privacy and how it protects other important values. Part C focuses on the crucial element of privacy definition – autonomy. It explains what autonomy is and how autonomous choices are related to consent. Furthermore, it discusses problems of consent, and shows how to exercise autonomous choice in respect of privacy process.

A The Scope – Personal Data Collection and Use by Service Providers

This Part presents the main concepts and actors, which is needed for the evaluation of the data privacy concept and, broader, the whole thesis. It explains what personal data are, how they relate to individuals, and who and how collects and uses those data. This, also, presents the scope of the thesis.

1. *Data and information*

Dictionaries often treat data and information as synonyms,[2] but these notions need to be distinguished. Information is a semantic concept, which can be understood as structured (or well-formed) data which mean something.[3] Data are tangible objects which can be conceptualised as quantified parts of (potential) information, represented in a digital world by

[1] Data processing is a collective term for operations performed on personal data (eg collection, storage, use).

[2] Eg Oxford English Dictionary.

[3] Floridi 2010, p.21; Wacks 1993, p.25; Albers 2014, p.222.

bits and their collections, and constituting larger parts, such as characters or records.[4] They need some structure, but what gives them meaning is the interpretation and understanding of a data user in a particular context and with a particular knowledge.[5] Knowledge is both a factor enabling interpretation, and a product of information processing (because factual, true information is a necessary precondition for knowledge).[6] Finally, if information and knowledge relate to individuals, they may provide a basis for decisions and actions which affect their positions.[7]

The development of Information and Communications Technology (ICT) has enabled the processing of an increasing amount of data, including those related to identifiable individuals – personal data. Technological advancement means that the Internet[8] is now a place for commerce, services, a backbone of business, and a medium of communication for approximately 3.5 billion individual users.[9] But, all online activities generate traces of data, for example, web searching generates browsing history, shopping or interacting on social networks produce histories of activities, mobile terminals generate streams of data related to location, detected networks, or readings from different sensors. As a result, humanity generates and accumulates enormous amounts of data. Schmidt claimed in 2010 that "in the world we create as much information in two days now as we did from the dawn of man through 2003".[10] Since then, the amount of data collected worldwide keeps doubling every two years (a yearly increase of 50 per cent), as presented in Figure 1. In parallel, the costs of keeping those data keep falling yearly by approximately 20 per cent.[11]

[4] For the reasons stated here 'data' is treated in this thesis as a plural noun. Although the dictionaries nowadays tend to present data as a mass, uncountable noun, data privacy (and data protection) laws and most of the relevant literature adhere to a more traditional view of a plural noun.

[5] Albers 2014, p.223; Wacks 1993, p.25.

[6] Floridi 2010, p.36.

[7] Albers 2014, p.223. Factual positions and legal positions, so their rights and obligations.

[8] The Internet is treated in this thesis as the global collection of interconnected networks, hence the use of it as a proper noun.

[9] International Telecommunication Union 2016.

[10] Siegler 4 August 2010.

[11] Based on data of International Data Corporation, Kleiner Perkins Caufield Byers 2016, p.195.

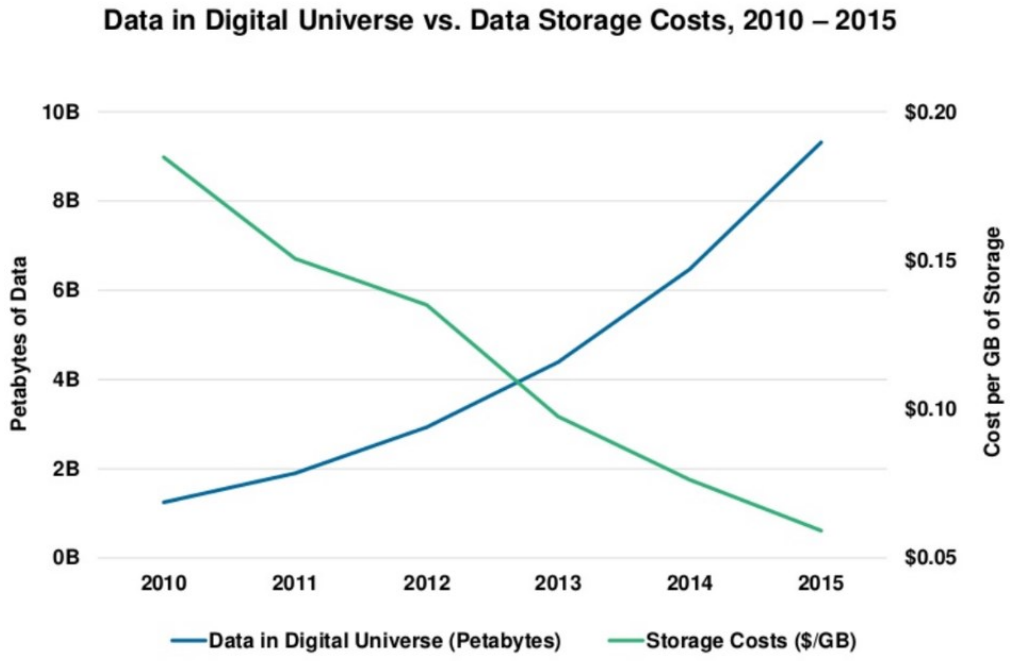


Figure 1 The surge of data, KPCB Internet Trends Report

2. *Individuals and personal data collection*

Personal data are defined through their relation to identifiable individuals called 'data subjects'.[12] Identifiability needs to be assessed in the context of the entity possessing the information/data and the set of possible subjects from which the individual is about to be identified.[13] So, whether an individual can be identified depends on the particular context and access to particular sets of other information. Because of this subjectivity, defining personal data (or information) in this manner brings some uncertainty for those who collect data. Sometimes, there will be a need to assess on a case-by-case basis how easy or how likely it is that the individual could be identified by the data holder.[14]

Also, personal data make up the identity of data subjects. Identity, besides its philosophical meaning as an exclusive perception of life,[15] is a subset of attributive values of an individual

[12] This is the legal definition of 'personal data' or 'personal information' which can be found in relevant statutory law in the researched jurisdictions.

[13] Pfitzmann and Hansen 2010, p.30.

[14] Eg Article 29 WP (WP 136) 2007, p.5.

[15] ICT changes the perception of identity, Floridi 2010, p.15.

which sufficiently identify this person within any set of persons (the opposite of anonymity).[16] So, it is effectively a subset of one's personal data which represents that individual in online interactions (eg 'login' and password, private key, or set of answers to security questions) and is absolutely critical for many online services (eg the bank). Also, for individuals it is critical to control a subset of data which proves (or maybe even determines) their identity. This is because losing this control may lead to 'identity theft', when someone's identifying personal data are used to commit crime (usually fraud). But individuals can have multiple identities composed of different personal data (eg a name, or a unique identifier assigned to a website viewer)[17] and often there is no clear distinction between identity attributes and 'mere' personal data (eg set of answers to security questions). This suggests that all personal data should be treated with similar care.

Processing of data takes place in a sequence of steps comprising creation (or generation), collection, storage (and aggregation), analysis, and use (which may involve transfer).[18] Data are created in electronic devices which are used by individuals, collected by a range of companies with an online 'presence' and then reused for different goals by other individuals, governments, or businesses. They may be categorised (based on the way they were obtained from the individuals) into volunteered data, observed data, and inferred data (ie derived from other data).[19] Observed data are gathered as a product of online choices of data subjects (eg visited websites,[20] clicked objects) or a by-product of their activity in the form of transaction or communication metadata (so, data about other data, eg IP address, location, data about transactions).[21] Many people may be unaware of how this processing takes place because usually those actions are not visible from their perspective.[22]

---

[16] Pfitzmann and Hansen 2010, p.30; section 2.7, ISO/IEC 29100:2011(E).

[17] Broader in Zuiderveen Borgesius 2016, pp.262–265; Narayanan 2011.

[18] Floridi 2010, p.5; Albers 2014, p.223; cf Solove 2006, p.490. Note that 'processing' covers all activities related to data.

[19] World Economic Forum and Bain & Company 2011, p.7.

[20] Terms 'visit' and 'site' from colloquial language are misleading. This is because the communications works in the opposite way. Computer code and data are downloaded from a server to a user device and the computer code is executed there.

[21] Whittington and Hoofnagle 2012, p.1345.

[22] Lessig ("The Law of the Horse: What Cyber Law Might Teach") 1999, p.511; Lipman 2016, p.7; although, increasingly aware of their own lack of knowledge and understanding, see Lips and Löfgren 2015, p.10.

Also, personal data may give different insights about individuals: their inherent characteristics (eg demographics), acquired attributes (past actions, relations), and individual preferences (interests).[23] All those data form profiles of data subjects.[24] Both the number of the traced individuals and the level of detail may be very high. For example, one of the biggest US data brokers, Acxiom collects information on 700 million customers worldwide and divides many of them into over 3,000 data segments.[25] Another data broker, Datalogix is a partner of Facebook in analysing online and offline behaviours of its over two billion users.[26] Such a large amount of data may help to automatically predict a wide range of individual traits and attributes, even those related to aspects of the personality, political views, emotions, sexual orientation, or beliefs.[27] Those are things which the individuals in question may not have intended to share.[28]

The intention behind commercial data collection is to build a knowledge base about individuals, because such knowledge has a value for those who would like to influence their behaviour. In fact, such databases of profiles can be analysed to target any messages which would appeal to particular individuals, depending on wishes of data holders and their customers. For example, this may be used for selling products to individuals or convincing them of ideas. As a result, those personal data are exposed for an indefinite number of potential users and uses. Such exposure generates tension, as it creates potential for manipulation and decreases personal security. Also, the possession of vast amount of personal data, describing traits which are not intended to be communicated to others, and collected to manipulate data subjects, gives data controllers significant power over individuals and may be considered as disrespectful or inhumane treatment.

---

[23] The Boston Consulting Group 2012, pp.35–36.

[24] A profile is a number of assumptions about the individual based on one's data, The Norwegian Data Protection Authority 2015, p.25.

[25] Federal Trade Commission 2014, p.8.

[26] Ibid., p.8.

[27] Kosinski, Stillwell and Graepel 2013; Kosinski and others 2016.

[28] The word 'share' is a well-crafted metaphorical framing excessive collection of personal data from positive perspective. Therefore, it will be used sparingly and usually in quotation marks.

For these reasons, as will be argued below, individuals need to control their own exposure to the view of others as they were used to do in a world which relied less on ICT. If individuals are to have such control, they need to control their personal data, because personal data contain information related to their attributes, which may be revealed to target them. Furthermore, recent research shows that people are increasingly concerned about not having control over data they provide online.[29]

Very large sets of data are often called 'Big Data'. This notion includes also methods of analysing them,[30] so it is a combination of technology and a specific process.[31] 'Big Data' are usually described through the '3V model': volume, variety and velocity.[32] The huge volumes of data coming from a variety of sources are being analysed at a velocity which is approaching real-time.[33] The goal is to infer from such datasets new correlations and trends (using statistical modelling or machine learning methods, for example) and instantly deliver results. These results may infer preferences of the individuals and predict their behaviour.[34] Such an approach to personal data processing changes a few paradigms. Firstly, data are automatically generated and analysed as streams and no longer processed in singular events/transactions. Also, data processing is often automated as to decision making and action[35] (eg automatic offers based on collected data, or adjusting environment in 'smart' homes[36]). So, control over those actions require control over data streams. Secondly, in a large dataset, even small amount of data which do not directly point to individuals may serve to identify them.[37] This impacts on the scope of data which needs to be controlled. Thirdly, the use of 'Big Data' changes the competition model of many businesses. This has huge implications for the economy as data are commercial assets and competition moves towards the control over vast amounts of data and ability to quickly analyse them.[38]

---

[29] Kleiner Perkins Caufield Byers 2016, p.209; TNS Opinion & Social (DS-02-15-415-EN-N) 2015, p.5.

[30] Mayer-Schönberger and Cukier 2013, p.6.

[31] Yeung 2017, p.119.

[32] Sometimes extended to 5V by including veracity and value.

[33] The White House 2014, pp.4–5.

[34] Federal Trade Commission 2016, p.2.

[35] 'Output automation', Spiekermann 2008, p.18.

[36] Adib and others 2015.

[37] Rubinstein and Hartzog 2016, p.713; More broadly, Ohm 2010, p.1723 ff.

[38] See Chapter III.

This leads to the next question in this chapter – who are the data controllers and how do they use personal data?

3. *Service providers, the use of personal data, and authorisation*

Data controllers are various types of entities that control processing of personal data in their activities.[39] There is a need to narrow down this broad group to those controllers who provide online services (service providers). This particular group of data controllers is characterised by the way their use of personal data is authorised and by the interests the processing serves.

In relations between data controllers and data subjects, data processing is authorised either by data subjects or by 'other means'. Processing is authorised by data subjects when they give their consent to the collection and use of data. Such consent may be either the acceptance of a contract or a separate consent to collect data. Giving this consent data subjects act in their own, individual interests. 'Other means' of authorising data processing are either references to legal rules, or to some societal needs or standards. In practice, this depends heavily on legal culture. For example, in the European Union all permitted legal bases for data processing are enumerated[40] (although some take the form of general clauses).[41] So, to some extent all are defined in law. It looks very different in New Zealand and Australia, where the legal bases for data processing are left undefined,[42] but, instead, law focuses more on limits for data collection[43] and use.[44] Within those limits there are particular purposes or limitations which depend on the existence of particular (usually public) interests. The Canadian law represents

---

[39] To avoid confusion the thesis does not introduce the term data processor, who, according to the EU Law (DPD, Article 2), may process personal data on behalf of the controller (who determines the purposes and means of processing).

[40] Eg DPD, Article 7; GDPR, Article 6(1); however, there are also other legal bases for processing 'special' categories of data.

[41] For example, "processing is necessary for the purposes of legitimate interest pursued by the controller or by the third party", DPD, Article 7(f).

[42] Those countries also abstain from defining 'data processing'.

[43] See principles 1-4, Privacy Act 1993, s 6; see principles 3-5, Privacy Act 1988 (Cth), pt 2 sch 1.

[44] See principle 10-11, Privacy Act 1993, s 6; see principles 6-9, Privacy Act 1988 (Cth), pt 3 sch 1.

a mixed model with an explicit demand for data subject consent (so individual authorisation), but with broad derogations. Table 1 gives some insight into types of authorisation with examples taken from data privacy statutes in the researched jurisdictions.[45]

Table 1 Types of authorisation of data processing (or collection, use) in the researched jurisdictions.

Authorisation by individuals	**Authorisation by other means**	
	legal needs	**societal needs**
• Consent; • Contract (including the phase before entering the contract and after its termination); • Employment contract.*	• Exercise of authority, action in public interest, law enforcement; • To comply with a legal obligation of data controller; • To bring claims (including claims in ADR systems), and to debt collection; • Security, fraud or money laundering prevention.	• Medical prevention; • Non-profit use by NGOs, foundations, political parties, trade unions; • Research, statistics, archiving; • Journalism; • Art, or literature; • Household or personal use; • Vital interest of data subject or third party; • 'Legitimate interests' of controller or a third party.**

* - employment contract is a *sui generis* category as data subjects have a different role (to provide labour);

** - mixed authorisation by society needs and by the needs of data controllers.

So, the 'other means' of authorisation, in Table 1, are usually based on the public interest, either explicitly formulated in the law to provide a legal system with some use of data or defined by the reference to their societal function. In each of these situations the authorisation of data subjects to use their data is not required.

Taking into consideration the above distinctions it is possible to present different types of data controllers processing personal data online as shown below in Figure 2.

[45] The author exercised some discretion in naming these categories and assigning to them specific actions. There may be other views.

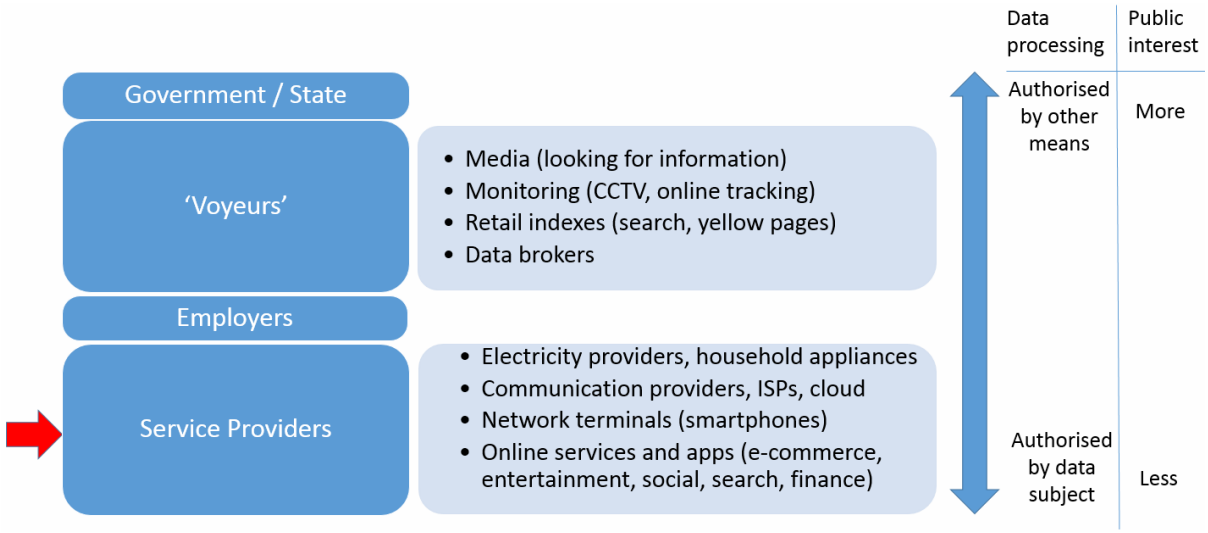


Figure 2 Entities processing personal data online.

This picture shows, on the left, groups of entities processing personal data related to online activities of the individuals, spread out on the continuum between individual authorisation and other means of authorisation. In such data processing, there will be a mix of interests of data subjects, data controller, and public. This third element, public interest, is stronger for the entities in the upper part of Figure 2. For example, state authorities normally process data in the public interest, which is authorised by law.[46]

The main purpose of this picture is to show who online service providers are, because this thesis focuses mainly on them. They are all providers of services and goods on the Internet who collect personal data in the course of their activities, having (primarily) their own, usually commercial, interest in doing so. And, as the picture shows, service providers use mainly individual authorisation. This is because the main interests which are at stake in these relationships are the commercial interest of data controllers, and interests of data subjects (to receive services, and the interest in their personal data which will be named in Part B, below).

Data controllers whom Figure 2 labelled 'voyeurs' collect personal data from available public sources. They are not providing online services, but, as will be shown in Chapter III, some of them occupy an important role in the online environment and may need to be regulated. Also, sometimes the same company may play different roles. For example, a firm providing search services such as Google is a service provider, but its indexing 'robots' or 'web crawlers' that

[46] But, they may also provide some additional services and use individual authorisation for collecting additional personal data.

collect virtually everything from the web are processing personal data as 'voyeurs'.[47] The same dualism may be seen in the case of media gathering information from any possible sources ('voyeurism') and providing their users with services based on those data. So, particular online companies may have different sets of personal data related to different interests and therefore to different obligations. Furthermore, different obligations may be related to the same dataset. This is, for example, the case of telecommunication metadata collected and processed on the basis of contract, but with legal obligation to be retained for public security. The existence of other interests limit the individual control over some sets of personal data.

Also, personal data may be used differently by service providers and, therefore, the potential implications of such uses for data subject may vary.[48] Typical activities related to data processing and their impact on the risk for data subject are presented in Figure 3.

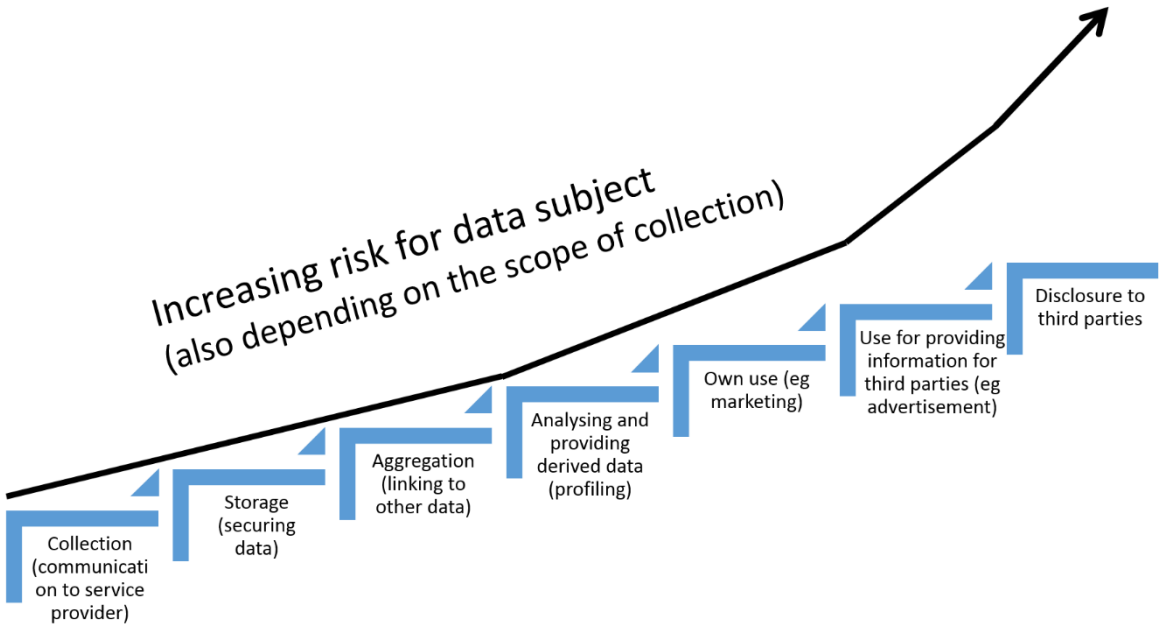


Figure 3 Data processing activities.

As shown in Figure 3, the mere collection and storage of personal data implies risks for data subjects. This is because those data may be lost by the data controller, for example, as a result of breaching their protection measures by hackers. Nowadays, such data leaks happen with

[47] Which is performed, allegedly, in the legitimate interest of the general public to enable them access to information, Case C-131/12 *Google Spain* [2014] CJEU, para.81.

[48] More details in Chapter III.

increased frequency and are a real problem for data subjects.[49] The level of risk depends on the scope of collection: the more data collected, the higher the risk.[50] This problem is even worse, because data subjects may not be sure what data are collected,[51] so they cannot properly assess the risks. When data are collected, the level of risk they pose depends on the way they are used. In general, the more they are aggregated (ie detailed and linked),[52] the more dangerous they are for individuals. This is because they may reveal more personal information for anyone who may gain access to them (service provider, third party, or potential 'attacker'). Furthermore, there are two particular actions of service providers which additionally increase the risks: profiling and providing third parties with personal data.[53] This is because profiling relies on evaluating personal data towards analysing and predicting individuals' behaviour,[54] which can reveal more information about them. And, communication of data to third parties increases the risk, because more subjects possess them and data subjects are vulnerable to the actions of all of them.

The actions described above which increase level of risks for data subject may be perceived as the potential levels of data control. This is because data subjects may want to be involved in making decisions which result in the increased risks to their (potential) detriment. So, they may prefer to avoid data collection at all, to avoid the risk. Or, they may decide to take the risk of collection, but disclose their data only for particular uses and particular service providers whom they trust and not to authorise further dissemination of their data to third

[49] Data controllers which were subject to significant data breaches recently are Sony, Ashley Madison, Anthem, Yahoo, eBay, JP Morgan Chase, Walmart, and the United States Office of Personnel Management.

[50] Cf with views that "increasing data use does not necessarily increase risk", Australian Government, Productivity Commission (No. 82) 2017, pp.11–12, which, however, seem to be substantiated by the increased use of anonymous data.

[51] Eg Sørensen 2016.

[52] Linked to particular data subjects. Note that aggregation of data from multiple individuals may also serve to increase their anonymity, but this is not the meaning used here.

[53] The black line in Figure 3 conceptualises the increase of risk, but does not attempt to precisely quantify it.

[54] Example of legal definition of profiling: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements", GDPR, Article 4(4).

parties.[55] These levels of data control will be important later in the thesis because they help to structure different uses of personal data.[56]

As all the basic information about data processing actors and their activities has been outlined above, it is possible to turn to describe the nature of the individual interests in personal data.

B Data Privacy

Such interests are usually labelled as privacy, but this notion remains undefined and problematic. So, this Part defines privacy in respect of personal data processing.

1. *Normative and non-normative accounts of privacy*

Individual interests in maintaining some level of social distance towards others (or separatedness) are traditionally called privacy. It may be rationalised in many ways: as distance setting derived from animal behaviour,[57] as a need to be safe from more powerful others,[58] protection of dignity,[59] need for a space for "taking off the mask",[60] or space to contemplate ideas,[61] or even protection from society imposing own ideas and practices as "tyranny of the prevailing opinion and thinking".[62] All those explanations also apply in the online environment. As will be shown in Chapter III, they may be even more relevant there. But, although the concept of privacy is universal and necessary for the proper functioning of human beings, understanding of exactly where the balance lies between private and exposed to public view is not only culturally dependent, but also very subjective, and dependent upon

[55] For example, in a survey 31 per cent of respondents disapproved of data collection by service providers while as many as 70 per cent disapproved of allowing third parties to use the same data. The Boston Consulting Group 2012, p.45.

[56] In Chapter VI.

[57] Westin 1984, pp.57–59.

[58] Mill 1859, p.3; see also this account from the perspective of biologist Peter Watts in IAPP MultiMedia 2014.

[59] Eg Warren and Brandeis 1890, p.205.

[60] Jourard 1966, p.310.

[61] Moore 2012, p.4; also, Socrates absorbed in solitary thinking in a portico in Plato's *Symposium*.

[62] Mill 1859, pp.13–14.

particular relationships.[63] Personal privacy decisions may vary by situation, time, nature of the information, culture, social expectations, and motivation.[64]

Perhaps this is the reason why privacy has no uniform definition. The discussion around privacy is often confusing because it refers to different understandings of this concept. Privacy was understood by different authors as a state (or condition),[65] an aspect of control,[66] a claim,[67] or entitlement, an umbrella term for resembling concepts related to the risk of harm,[68] or a right.[69] Looking at this list, there is little doubt about why it is hard for the theorists to agree on one definition – they describe different concepts and mix what *is* with what *ought to* be.[70] To make this discussion easier, the thesis discerns three categories of concepts as presented by von Wright: notions of human acts (needs, desires, and interests), values, and normative concepts.[71] In other words, it will distinguish what privacy *is*, from what privacy is *worth*, and from what privacy *ought to* be.[72]

This chapter concentrates on non-normative accounts of privacy, so it describes the interest (and the will of individuals) and assesses the *worth* of such interest. Therefore, *privacy* is described here as the interest which is *worthy* of protection[73]. This is distinguished from how this interest *ought to* be protected.[74] Some legal means for such protection will be called the *right to privacy*. The actual protection depends on the 'strength' of privacy interest (so, also on its definition), but also on the relative 'strength' of other legitimate interests against which privacy is balanced (if there is a conflict between those interests and privacy).

---

[63] Altman 1977; Moore 2010, p.55; Solove 2008, p.48.

[64] Nissenbaum 2004, p.156.

[65] Eg Inness 1996, p.140; Parent 1983, p.269.

[66] Eg Westin 1967, p.7; Moore 2008, p.420.

[67] Westin 1967, p.7.

[68] Solove 2008, p.45 ff.

[69] Eg Warren and Brandeis 1890.

[70] More about sliding between those meanings in Moore 2008, p.418.

[71] von Wright 1963, pp.6–7.

[72] This approach does not aim to discuss the concepts (or boundaries) of normative ethics. This classification of concepts is rather used to distinguish the evaluative from prescriptive.

[73] Cf. DeCew 1997, p.53.

[74] See the following chapters.

2. *Data privacy as informational self-determination (autonomy)*

The interest in data privacy is defined in this thesis as informational self-determination (or autonomy). This definition was developed in 1983 by the German Federal Constitutional Court (*Bundesverfassungsgericht*, or BVerfG) in a landmark *Census Act* case.[75] The Court defined the right to informational self-determination as the right which "guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data".[76] In other words, privacy is defined in this thesis as the ability to make one's own decisions about the disclosure and (separately) use of one's personal data. In 2008 in the decision on the *North-Rhine Westphalia Constitution Protection Act* the BVerfG further extended the protection of personal data by recognising another fundamental right to the "guarantee of the confidentiality and integrity of information technology systems".[77] The reason for this decision was to protect data in IT systems used by the users "as his or her own".[78] The interest recognised in this decision (the interest in confidentiality and integrity of information in IT systems) is here treated as a part of informational self-determination,[79] because it relies on essentially the same – deciding as to the disclosure and use of personal data, regardless of their location. The concept of informational self-determination is analysed below, starting from the arguments given by the Court.

The BVerfG grounded the right to informational self-determination on the fundamental values of dignity and 'worth' of individuals. These individuals, they said, function as members of society through individual self-determination. The Court recognised that dignity and 'worth' are protected through a general right to free development of one's personality,[80] which in this case included the right of individuals to decide for themselves, in principle, when and within what limits personal matters are disclosed.[81] According to the Court, this was threatened by

---

[75] *Census Act* [1983] BVerfG; a summary in English is in Bröhmer and Hill 2010, p.143 ff.

[76] Bröhmer and Hill 2010, p.148.

[77] *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG.

[78] Ibid., para.206.

[79] So, slightly different than did BVerfG. More in Chapter VII.

[80] A positive liberty formulated in Article 2.1 of the German Basic Law.

[81] Cf the definition of privacy in Westin 1967, p.7.

new technologies of data collection, which could be used to assemble an essentially complete personality profile without "giving the party affected an adequate opportunity to control the accuracy or the use of that profile".[82] A similar profile, giving "insight into significant parts of the life of a person" and providing "a revealing picture of the personality" can be constructed (or accessed) by breaching the confidentiality or integrity of the individuals' IT systems by third parties.[83] Such a profile, according to the Court, might be used for consultation or manipulation which can affect the individuals concerned. The individuals, the Court recognised, should be free to make plans or decisions in reliance on their personal power of self-determination. So, they should be able, to some degree, to ascertain "who knows what about them".[84] This is not possible when data are under the control of others or their own IT system is surreptitiously accessed by others. Without such ability, people would avoid standing out through any unusual behaviour, because this could be recorded and disclosed to unknown recipients. This, the argument goes, would restrict personal development and would be detrimental to the public good. In such a way, the Court also recognised that informational self-determination is a prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members.[85]

This construction of a privacy definition is not a traditional one. Most privacy definitions use the construction of negative liberty (so 'freedom from'), which is probably a legacy of Warren and Brandeis' definition of the right to privacy as "the right to be let alone".[86] In this view, privacy may be seen as hiding or protecting some private sphere from the eyes of others. For example, Moore recognises the condition of privacy as when an individual freely separates herself from her peers and restricts access.[87] Privacy is explained in a similar manner by Moreham as a desired inaccess.[88] Such an approach usually points the discussion towards consideration of which spheres should or should not be concealed, for example, feminists claiming that privacy was used to conceal the sphere of women's subordination and domestic

[82] Bröhmer and Hill 2010, p.147.

[83] *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG, para.203.

[84] Bröhmer and Hill 2010, p.148.

[85] Ibid., p.148.

[86] Warren and Brandeis 1890.

[87] Moore 2008, p.421.

[88] Moreham 2005, p.636.

violence.[89] Posner, in a famous critique of privacy, claims that individuals should not have the right to conceal material facts about themselves, as it misleads others and allows sellers to make false or incomplete representations.[90]

In contrast with those views, informational self-determination is an account of privacy which describes it as a 'freedom to'. This acknowledges the agency of the individuals to make their own decisions about the disclosure and further use of data, which widens the scope of their liberty. For example, in this view, others should not only refrain from knowing private facts (data) about individuals, but also allow them to exercise their decision-making abilities (or freedom), to decide which facts (data) are accessible. This shifts the emphasis away from describing individuals' private spheres to describing their ability to make their own decisions, that is, their autonomy.[91] This definition was built upon control-based definitions of privacy according to which individuals should be able to determine (or control) the communication or circulation of their personal information.[92] It evolved from the existence of choice (or control) of the individuals as to the first communication of their personal information (to data controllers)[93] to control of how the information could be further used and distributed (by data controllers). This is, after all, a natural way people treat private information – they attach conditions to the use of such information when they pass it to others, eg tell others to keep it to themselves, or to use it in a specific way.[94] Informational self-determination follows this natural behaviour. It says that individuals should have the ability to make their own decisions as to the first communications and subsequent use of data. The decisions of individuals should be in principle autonomous and they should be able to determine 'who knows what about them'. It follows then that data privacy is a data subject's autonomous control over personal data described by setting its goal – the ability to determine the actual use of personal data. The formula 'to determine who knows what about a data subject' describes both the required

[89] Allen 1999, p.741.

[90] Posner 1978, p.399.

[91] More in Part C. Cf critique of such approach, Cohen 2012, p.110 ff.

[92] "Claim to determine when, how, and to what extent personal information should be communicated", Westin 1967, p.7; "control over knowledge about oneself", Fried 1968, p.483; "ability to control the circulation of information", Miller 1971, p.25.

[93] "Determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others", Warren and Brandeis 1890, p.198.

[94] Privacy Management Theory, Petronio 1999.

prerequisite and effect of informational self-determination, and will be used as a test for the existence of its breach in the next chapter.

The formulation of privacy as informational self-determination empowers individuals by giving them more autonomy in respect of their data both in scope of subject-matter and intensity of such control. Such control could be exercised as direct control over data, or indirect control by the means of data controllers and their accountability.[95] This responds to the challenge posed by the online environment in which "day-by-day drops into the ocean of data … are assembled to construct user profiles, where even seemingly innocuous data can reveal sensitive information".[96] The BVerfG recognised this stating that all types of personal data should be treated with the same attention because "unimportant data no longer exist" in the context of ICT.[97] This is different from a 'traditional' understanding of privacy in which information needs to have a private nature, a merit of being related to some private sphere of the individual.[98] But, if any piece of personal data has potential to reveal sensitive information because of the way data can be nowadays processed in the ICT environment,[99] that piece of data needs to be covered by the account of privacy. This is because that piece data is a 'raw material' for creating sensitive information. It may be not possible to control information,[100] but it may be possible to control the raw material for creating it. So, if data subjects need to have their values protected, possibly all their personal data need to be subject to some form of control by them.

The need for this control may be derived from the privacy values. Those values and their importance will be described in the following chapters as they impact on the scope of the problem and necessary control 'mechanism'.

---

[95] Spiekermann 2008, p.31. Also, Chapter III.

[96] European Data Protection Supervisor ("Report of workshop on Privacy, Consumers, Competition and Big Data") 2014, p.5.

[97] Bröhmer and Hill 2010, p.149.

[98] For example, in the jurisprudence of the European Court of Human Rights. Eg *Amann v Switzerland* (*2000)* ECtHR, para.69. More in Chapter VII. Also, Gellert and Gutwirth 2013, p.526.

[99] Cf the idea that systematic collection and storage of data gives them a merit of being 'private', *Rotaru v Romania* (2000) ECtHR, para.43.

[100] As it includes the meaning created by understanding data in someone's mind.

3. *The importance of privacy values*

The values behind privacy are non-normative descriptions of how privacy can be valued, or what worth can be assigned to it.[101] There are two main dimensions in which privacy can be valued: an economic (tangible), and a personal (intangible) one. There seems to be discussion in the literature as to whether privacy has any value by itself (ie it is a final value), or whether it is 'only' protecting other values, having by itself only an intermediate (or instrumental) value.[102] This is not just a theoretical point because people party to bargains in which they pay with their personal data have to value their privacy on the spot. What they assess at this point is mainly the final value (of privacy or data by themselves), while the risk introduced by data processing to other values seems to be out of the scope of their privacy decisions.[103] The problem of valuing data relies on the inability to assess and control privacy risks, information asymmetry, and bounded rationality,[104] but also on the inherent problem of expressing intangible values protected by privacy in economic terms. What are those intangible values?

The BVerfG in its decision pointed to the dignity of individuals, and their 'social worth'; the ability to participate in societal interaction as reasons for valuing privacy. This points to two aspects: internal and societal. The internal aspect is that privacy is indispensable for moral integrity, identity, individuality, having a sense of one's own worth, or searching for meaning of life. Ultimately, privacy is needed for dignity and autonomy of human beings. Dignity is also mentioned by the 'inventors' of the right to privacy, Warren and Brandeis as a "spiritual value" of privacy[105] or "inviolate personality".[106] Many other authors are of a similar view,[107] which may be traced to the Kantian recognition of persons as ends in themselves.[108] In this sense, the autonomy argument is very similar, although it points to a more 'dynamic' attribute

---

[101] There may be other views on the nature of values. Both interests and values may be seen as normative concepts, eg von Wright 1963, pp.155–156.

[102] Rouvroy and Poullet 2009, p.50; Solove 2008, p.84; Farrell 2012, p.252; Acquisti, Taylor and Wagman 2016, p.447.

[103] Acquisti, Taylor and Wagman 2016, p.447; Whittington and Hoofnagle 2012, p.1346.

[104] Whittington and Hoofnagle 2012, p.1346.

[105] Warren and Brandeis 1890, p.197.

[106] Ibid., p.205.

[107] Bloustein 2003, p.42; Moreham 2008, p.238.

[108] Fried 1968, p.478; Laurie 2002, pp.84–85.

of human beings as choice makers, steering their own course through the world, their creativity and development.[109]

Importantly, those values are *inalienable* from the person. That is to say, dignity or autonomy are internal and inherent to human beings,[110] so they cannot be detached from the data subject as can be, for example, property entitlements. Some say that privacy is natural right inherent to a person,[111] Kantian moral entitlement to ourselves, or a fundamental right,[112] which captures the same idea that privacy cannot be surrendered or given away (like property). This is not a limitation of the capacities of the individuals, but an extension of liberal theory to secure the sovereignty of the individual in a new type of society.[113] Such 'classical' views have interesting variants relating to the protection of individuals in the online environment. Floridi describes information as a *constitutive* part of someone's personal identity and individuality.[114] So, in his view, privacy is a protection of a person in the 'infosphere' and taking away personal information is akin to kidnapping that person. This resonates with the idea of Habeas Data rights in many Latin America countries, which guarantee individuals basic procedural means for challenging actions of others regarding their personal data (per analogiam to Habeas Corpus).[115] This seems to be intuitive, that if personal data are constitutive to the identity of individuals, the control over data should be a strong one. Furthermore, such control may even be similar to the control of other constitutive parts of people: over own body and mind.[116]

Privacy protects also external social value. Such social value may come from the idea that

---

[109] Benn 1984, p.229; Gavison 1984, pp.361–362; Dworkin 1988, p.104; also, well-being needed for self-development in Jourard 1966, p.318.

[110] Eg preamble to Universal Declaration of Human Rights 1948.

[111] Richardson 2016, p.13.

[112] Schneier 2015, p.201.

[113] "In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign", Mill 1859, p.22.

[114] Floridi 2005, pp.195–196; more broadly in Floridi 2014, pp.118–124.

[115] Such rights exist on the constitutional level and provide access, correction, ensuring confidentiality, and means to remove some of data; more details in Guadamuz 2001; see also discussions within the United Nations, Rodotà 2009, pp.81–82.

[116] Cf Mill 1859, p.22.

privacy is invaluable for creating relationships. As Fried says: "[t]he man who is generous with his possession but not with himself can hardly be a friend, nor can the man who shares everything about himself with the world."[117] In such a view privacy is protecting the capacity to enter into closer relationships: friendship, love, and trust.[118] This is similar to protecting dignity, however, the emphasis shifts to a social life which is, in this narration, constitutive to the personhood. This argument may be extended to professional relationships, like a psychotherapist, employee, or student.[119] It may be extended even further towards virtually every kind of social participation, even interactions with strangers.[120] All of this may constitute a defence of privacy from the communitarian perspective, which understands individuals as "members of this family or community or nation or people, as bearers of this history, as sons and daughters of that revolution, as citizens of this republic".[121] In a liberal view, democratic society needs citizens making their own reasonable choices as constituents and decision makers.[122] This may be called the necessary moral autonomy of citizens,[123] or internal dimension of society which has to be able to control the government.[124] BVerfG raised the same point, explaining the value behind informational self-determination. Paradoxically, treating privacy in an overly 'liberal' way (trading it) restricts the freedom of individuals and liberal society.[125]

So, how is the conception of informational self-determination underpinned by privacy values put into practice in the online environment?

---

[117] Fried 1984, p.211.

[118] Reiman 1984, p.314; Fried 1984, p.205; also, Dworkin 1988, pp.24–27.

[119] Roessler and Mokrosińska 2013, pp.780–781.

[120] Ibid., p.781 ff.

[121] Sandel 1998, p.179; similar approach in Bernal 2014, p.27; cf also views other than Cartesian, for example, an African view of human is "I am because we are, and since we are, therefore I am", Mbiti 1969, p.106.

[122] Schwartz 1999, pp.1647–1658; Simitis 1987, p.733 ff.

[123] Gavison 1984, p.369.

[124] Solove 2007, p.763.

[125] Cf the view that liberal theory is incapable of protecting privacy, Yeung 2017, pp.130–131.

4. *Online privacy as a process of controlled self-revelation*

Data privacy understood as informational self-determination is a process of controlled self-revelation. This privacy process may be described as an ongoing, dynamic interaction with others in which people sometimes make themselves accessible to others and sometimes close themselves off from them.[126] Such an understanding was developed by Petronio into Communication Privacy Management theory.[127] This theory explains that people dynamically manage their privacy in constant tension between concealing and revealing information about themselves. On the one hand, they feel that they are 'owners' of their information and should be able to control it even when it is being communicated. On the other hand, they disclose information to others to form or maintain relationships with them. To control what is revealed, they negotiate and coordinate various privacy rules (in communication), which depend on many individual factors. People would like to control privacy differently with various partners depending on the perceived benefits and costs. It is selective because information appropriate in the context of one relationship may not be appropriate in another.[128] In this approach, privacy is the subjective and complex process of maintaining some control over one's information and its availability to others.

Such a perspective corresponds with both the view of privacy as informational self-determination presented in the previous section, and with the description of contemporary online data processing in which data are being generated as streams rather than in particular interactions. If individuals should be able to determine 'who knows what about them', they have not only to assess the information which is to be revealed, but also the information which has been revealed previously. This requires capacity to 'look back'. But, treating privacy as a process requires also the capacity to 'look forward', and, therefore, to plan. The goals of singular transactions (eg data transmissions) should be assessed within the framework of goals and successes of a long-term process.[129] Setting long-term goals requires describing and adopting some level of exposure towards others and deciding upfront about how data streams should be collected and used. This requires language (or a framework) in which it would be

---

[126] Altman 1977, p.67.

[127] A complete account of which seems to be in Petronio 1999; the latest update can be found in Petronio 2013.

[128] Schoeman 1984, p.408.

[129] Similarly, "contracts can be transactional or relational", Kim 2013, p.31.

possible to describe privacy decisions and further change ('renegotiate') them in case any changes to the level of exposure are needed. Those levels of exposure may be different for different cultures, personalities and goals in individuals' lives. For example, a celebrity would have an extremely different approach to privacy than a judge deciding criminal cases.

In the process of privacy where data are generated as streams, singular consent is either completely impractical (as it forces the individual to decide about each operation) or deprives individuals of control over their level of exposure (when it serves for blanket authorisation of future actions). But, if it were possible to provide control over privacy processes in which individuals could have an overview of their data and could make decisions about their goals regarding their collection and use, this could allow them to exercise their informational self-determination. This seems to be the way in which they could participate in social discourse and have an opportunity to develop their own individual way of life.[130] So, there is a need to develop the model of control which gives the individuals those capacities regarding their privacy processes. To do this, it is necessary to discuss the role of autonomy and explain how autonomy (and control) is related to the privacy process. This is done in the next Part.

C Autonomy and Consent in the Privacy Process

1. *Autonomy and consent*

'Self-determination' is another word for autonomy, the term derived from the Greek 'autonomia', self-rule of cities making their own rights. This concept of self-governing states may be extended to self-governing persons, however, there are multiple ideas of what this could mean.[131] Beauchamp and Childress explain that on a general level, there seems to be agreement between theorists that autonomy requires conditions of liberty (at least independence from controlling influences) and agency (capacity to action).[132] The rationale for autonomy is the recognition that every human being is an end in itself, determining his or

[130] Cf Simitis 1987, p.734.

[131] Buss 2016; Dworkin 1988, p.13; Benn 1984, pp.241–242; Beauchamp and Childress 2013, p.102.

[132] Beauchamp and Childress 2013, p.102; similarly, Reath 2006, p.155; cf also two models: freedom model and authenticity model, Faden and Beauchamp 1986, pp.237–238.

her own destiny.[133] So, autonomous persons are those who have the capacity to be independent and govern their own actions (or, be in control).[134] But, capacity to act autonomously is distinct from acting autonomously (so, in a way which reflects those capacities),[135] as it may be observed when, for example, autonomous data subjects do not read Terms and Conditions (T&Cs) of the online services and agree anyway. As described above in Part B, autonomy as the capacity of a person is the value protected by privacy. But here the focus is on autonomous actions, making (autonomous) decisions by the individuals as regards the disclosure and use of their personal data. A large part of the following discussion is based on the literature related to medicine, as the concept of autonomous choice and informed consent came to data privacy from medical ethics.[136]

Autonomous actions, as set out in the widely accepted work of Faden and Beauchamp[137] must fulfil three conditions. They must be:[138]

(1) intentional;

The action must correspond with the actor's conception, although planned and materialised outcomes may differ (eg foreseen but undesired). This criterion is 'binary', ie the intention exists or not;

(2) with understanding;

Understanding may be achieved only to a substantial degree, as everyone has a different capacity to understand. Also, there may be deficiencies in the communication process;

---

[133] Such moral grounds were built by Immanuel Kant, Schneewind 1998, p.483; cf O'Neill 2002, p.92; there are other perspectives, for example, from the communitarian perspective autonomy is not a definitive value, eg Sandel 1998, pp.179–181; also, Bernal 2014, pp.46–47; also, the approach mixing liberal and communitarian view, Agich 1993, p.31.

[134] Faden and Beauchamp 1986, p.8; also, to determine by themselves the course of their lives, Raz 1986, p.407.

[135] Faden and Beauchamp 1986, pp.8, 237.

[136] Neil C Manson and O'Neill 2007, p.4; Kosta 2013, p.111.

[137] Mainly in medical ethics and law, but the same concept of autonomous actions can also be seen in data privacy, Schermer, Custers and Hof 2014, p.172; Kosta 2013, p.132; Brownsword 2009.

[138] Faden and Beauchamp 1986, p.238; also, Beauchamp and Childress 2013, p.104; cf other condition of 'authenticity' – conscious identification with one's motivation, Dworkin 1988, p.81; such a condition, however, may be hard to operationalise, as, for example, stopping on a red light might not be perceived as autonomous, Faden and Beauchamp 1986, p.263.

(3) without controlling influences (non-controlling);

Not all influences are controlling. The authors discern categories of coercion and manipulation which may give individuals' autonomy varying degrees of limitation.

The important conclusion from this is that autonomous choice cannot be assessed using binary values. This is because an act can be autonomous 'by degrees' as a function of conditions of understanding (2) and non-controlling (3). As regards to the understanding, the line between a substantial and non-substantial degree of understanding may appear arbitrary and must be determined in light of specific objectives, such as meaningful decision-making.[139] This is a challenge in the online environment as it is new for its users and most actions related to data are performed in the ICT systems of service providers.[140] Also, not every external influence is controlling, and therefore damaging to autonomy. There is a substantial margin between coercion and persuasion and it is necessary to draw the line of what is acceptable in a specific case.[141] In this respect, it is worth noting that autonomous persons can submit to the authority of government, religion or another community as long as they exercise their autonomy in choosing to accept it.[142] Furthermore, there are canons of reasoning, norms of conduct, and standards people acquire by the means of others.[143] Also, values like loyalty, love, friendship, and commitment do not conflict with autonomy, as they are self-imposed.

This individual freedom, however, should be understood slightly differently in respect of personal data. This is because Faden and Beauchamp's theory devised for the patient-doctor relationship presupposes that without the controlling influence from the doctor (so with 'freedom from'), the patient is the only one who has control over their own (internal) decisions and actions. So, the less controlling the influence of the doctor, the more control the patient has. But, personal data are located externally to data subject, and, when considering autonomy over data, one's control over data located somewhere in the ICT environment of the online service providers cannot be presupposed in the same way. This is because the less controlling the influence of service provider does not mean more control for the data subject. So, the 'non-controlling condition' should mean something more in relation to personal data; it should

[139] Beauchamp and Childress 2013, p.105.

[140] See Chapter III.

[141] Faden and Beauchamp 1986, p.259.

[142] Beauchamp and Childress 2013, p.105; but, in some autonomy theories this is questionable, Buss 2016.

[143] Dworkin 1988, p.12.

include the actual ability to make decisions about those data and communicate them to service providers. This seems obvious if we consider synonyms of autonomy: self-governance, self-determination. Also, this is coherent with the view of personal data as being crucial (if not constitutive) to the identity of individuals. Therefore, the 'non-controlling condition' in relation to data has to be more than just a lack of controlling influence by the data controller; it needs to be replaced by freedom in providing one's own control over data exercised by data subject ('freedom to'). Such autonomy-based freedom should give an adequate range of options and autonomous capacities to choose between them.[144] Only in such a way is it possible to achieve informational self-determination.

Autonomous action may, in particular, have a form of an autonomous choice, which may, in particular, have a form of (informed) consent.[145] A decision to consent is the final element of several actions in which some specific proposals and information (disclosure) are provided by the party seeking consent (a doctor or data controller), the individual having competence for giving consent[146] comprehends this proposal, and, finally, gives consent acting without controlling influence.[147] So, in data privacy, consent is an act of *autonomous authorisation* to the terms of data use prepared and proposed by data controller. Therefore, it should conform to the conditions of validity discussed in previous paragraphs. So, it should be intentional, and given with understanding and without controlling influence (and, as discussed, with control of one's own data). By authorising (potentially intrusive) actions of another the individual waives prohibition of those actions.[148] Furthermore, the crucial element in authorisation is that the person who authorises "uses whatever right, power, or control he or she possesses in the situation to endow another with the right to act".[149] This is related to assuming by the individual in question the responsibility for the actions taken by the other party regarding the presented (in the case of consent) course of those actions.[150] In other words, *volenti non fit*

[144] Cf Raz 1986, p.425.

[145] Faden and Beauchamp 1986, p.277.

[146] This means usually some additional legal constraints on effective consent, such as minimum age.

[147] Faden and Beauchamp 1986, p.275; Kleinig 2010, p.9.

[148] It is well seen in medical law, where consent to medical treatment is necessary to waive the prima facie illegality of the act infringing on someone's bodily inviolability.

[149] Faden and Beauchamp 1986, p.280.

[150] Ibid., p.280.

iniuria,[151] so no injury is done to a consenting (willing) person. This requires the individual giving consent to trust the other party, which will be discussed later in this thesis.[152]

A data subject's consent is often used in data privacy as a method of individual authorisation.[153] It usually takes the form of authorising the collection and use of data for specific purposes (or uses).[154] Notwithstanding its importance, it is only a *procedural* tool, which depends on substantive entitlement possessed by the data subject (the entitlement to informational self-determination). So, consent may not be necessary when there are reasons to process data in the public interest which outweigh that of the individual.[155] Also, consent is not the same as autonomy or autonomous choice.[156] This is a detail which seems to be not fully discussed so far by scholars. Consent procedure is not the *only* way to autonomously authorise the use of one's data. There may be other means to authorise data processing by individuals. The Privacy Management Model discussed in this thesis[157] is one of the alternatives. Knowing what consent is, it is possible to describe its problems.

2. *Problems of consent in respect of data privacy*

Consent is as an expression of informational self-determination[158] which empowers individuals to some extent[159] to make decisions about themselves.[160] The assumption is that consent ensures that the information practices of data controllers take account of the interests of data subjects who control the use of their personal data.[161] Also, consent is used by individuals according to the free market principles to agree to the contractual price for their

---

[151] "Nulla iniuria est, quae in volentem fiat", Ulpian, *On the Edict*, Book 56. Also, a defence in tort law, eg *Titchener v British Railways Board* [1983] UKHL 10.

[152] In Chapter IV.

[153] See Part A.

[154] Eg DPD, Article 6(b); OECD Guidelines 2013, s 9.

[155] 'The Fallacy of Necessity' in Brownsword 2009, p.85.

[156] Cf the views about overuse of consent, O'Neill 2002, p.90; Laurie 2002, p.206.

[157] In Chapter IV.

[158] Kosta 2013, p.140; Schermer, Custers and Hof 2014, p.174; cf Zanfir 2014, p.239.

[159] They only respond to proposals framed by others.

[160] Solove 2013.

[161] Bellamy and Heyder 2 July 2015.

personal data.[162] As indicated above, that use and importance of consent vary in the researched jurisdictions and so do the particular legal obligations related to that use. In general, its role is much more important in Europe,[163] important but more flexible in Canada,[164] less prominent in Australia,[165] and rarely used in New Zealand.[166] The basic concept of consent includes all characteristics described in the previous section: intention, non-controlling, understanding, and capacity.[167] Some authors point out, additionally, that consent needs to be specific to a given course of action,[168] which may also be seen as the requirement of a service provider's proposal, as discussed in the previous section.[169] Interestingly, these conditions seem to correspond only with some of the problems described within the next paragraphs.

The literature recognises various problems with consent. Firstly, consent seems to be not properly informed, as people do not read and understand privacy policies. Schermer, Custers, and van der Hof call it "consent transaction overload".[170] There are too many consent requests and reading them is a Sisyphean task. McDonald and Cranor calculated that to read all the privacy policies just once a year the individual would need on average 40 minutes a day (of the average 72 daily minutes online).[171] Furthermore, people lack the capacity to understand privacy policies. Bernal suggests that the text of the policy is usually complex and full of legal terms, because it was written by lawyers and for lawyers.[172] However, while detailed privacy T&Cs are unreadable, a summarised label is not helpful because of the lack of practical details.[173] Therefore, this problem is difficult to resolve.

---

[162] Nissenbaum 2011, p.34.

[163] Ie in the EU, consent is anchored in Article 8 of the ChFREU, and is one of the legal bases for data processing, eg DPD, Article 7(a).

[164] PIPEDA, s 7, Principle 3, and ss 4.3.3 - 4.3.7 sch 1.

[165] It is required for collection and use of sensitive data, Principle 3, Privacy Act 1988 (Cth), sch 1.

[166] Not used as a method of individual authorisation of processing, but consent is used to authorise eg some additional activity of data controller. See Principle 10(b), Privacy Act 1993, s 6.

[167] Eg Article 29 WP (WP187) 2011, pp.11–21, 27–28.

[168] Ie it should clearly specify the action, cannot be a blanket one, Schermer, Custers and Hof 2014, p.172; Article 29 WP (WP187) 2011, p.17.

[169] And, maybe a requirement to enter into a valid contract, if T&Cs are an offer.

[170] Schermer, Custers and Hof 2014, p.176.

[171] McDonald and Cranor 2008, pp.563–564.

[172] Bernal 2014, p.37.

[173] Nissenbaum 2011, pp.35–36.

Secondly, there seems to be a problem with absence of meaningful choice for customers, which could be linked to the criterion of non-controlling. Schwartz and Nissenbaum claim that data subjects' choices are not free due to the agreement on a 'take it or leave it' basis.[174] Furthermore, users do not have a realistic alternative for the major service providers, such as Facebook or Google.[175] Also, data subjects face high switching costs and data cannot be transferred to another service. Even if it was possible, a strong 'network effect' exists caused by overwhelming majority of users subscribed to the 'main' service providers.[176] Some authors speak straightforwardly that the big Internet service providers are monopolies.[177] Therefore, the argument goes, people are coerced to use their services.[178]

Thirdly, rational choice seems to be impossible in respect of online services. This argument challenges the whole concept of using consent for individual authorisation. People may be unable to make a rational trade-off between the privacy risk and economic benefit, even if they have choice and have read and understood the privacy policy. One reason for this is the problem of the complexity of choice due to the data aggregation as highlighted by Solove[179] and Zarsky.[180] It may be impossible to manage data that people reveal because they consist of thousands pieces of information revealed in isolation to different companies and in particular contexts. Others argue that the shift in technology towards automatic data generating and processing makes impossible to consent to each particular activity alone.[181] Consent, then, may not be the appropriate authorisation method for the online environment.

Indeed, consent, as the main mechanism for individual authorisation, has serious problems with meeting the challenge posed by Internet services. Because of the problems described above, online consent is treated by many people as a burden, a pure formality, without

---

[174] Schwartz ("Internet Privacy and the State") 2000, p.825; Nissenbaum 2011, p.35.

[175] Koops 2014.

[176] Whittington and Hoofnagle 2012, p.1365.

[177] Kuner and others 2014.

[178] For economic aspects of online services see Chapters III and V.

[179] Solove 2013, p.1890.

[180] Zarsky 2002, p.15.

[181] Cate and Mayer-Schönberger 2013, p.71.

connection to the 'real-world' sense of 'consent'.[182] Bombarded with complex consent requests which give little choice, they give their consent for personal data processing without even reading the terms of the agreement, at the same time declaring that privacy is a real issue of concern.[183] Similarly, service providers treat consent as purely formal exercise of collecting the records of individuals' clicks linked with the current versions of information provided for them. For them, this is the last obstacle to benefit from personal data and the whole exercise is needed to remove the legal risk. Also, they often face the need to collect additional consents for new services. So, consent is a burdensome mechanism to use in the online environment and may be seen as losing the conditions of validity (eg understanding, non-controlling).

Such a situation where consent loses the conditions of its validity is undesirable for both data subjects and data controllers. If there are no other bases for processing, the lack of legality of consent may mean that the processing is invalid,[184] and, data controllers may have to face legal consequences which may include heavy penalties.[185] Consequently, data processed without legal basis cannot be used. For data subjects, lack of valid consent poses the problem of a lack of control over their online identities and increased risk of harm.[186] This overall problem is a failure of consent. One of the reasons for this is that consent is not an adequate means for exercising individual autonomy in a process.

3. *Autonomous choice in respect of privacy process*

Consent is a good authorisation tool for singular events, but it is inadequate for making autonomous choices regarding data processing activities which have the form of a privacy *process*, an ongoing interaction between data subject and data controller. This is because the capacity to act autonomously with respect to a process is different than with respect to singular events. This has already been recognised in biomedical research where the concept of 'dynamic consent' was coined.[187] As recognised above, a privacy process requires methods of

[182] Bernal 2014, p.36.

[183] Madden 12 November 2014; Lips and Löfgren 2015.

[184] Schermer, Custers and Hof 2014, p.172.

[185] Eg GDPR, Article 83.

[186] Details in Chapter III.

[187] Kaye and others 2015; Wee, Henaghan and Winship 2013; also, Whitley 2013, p.171 ff.

control capable of controlling its dynamics: some privacy 'language' (or framework with multiple options) capable of describing privacy actions; methods of changing/adjusting decisions; capacity to reflect based on the outcome of the previous steps of the process (as trust depends on previous experiences); and capacity to 'look forward', and therefore plan the process for a longer term.[188] Such a toolbox should provide individuals with autonomous choices.

So, the elements of autonomous actions need to reflect characteristics of a process. That is to say, for the understanding criterion individuals should have an opportunity to comprehend data processing activities and be able to take into account all data which were collected (so, preferably to 'see' them) or are about to be collected. Subsequently, in respect of intention and specificity of consent, processual thinking requires the ability to plan in the longer term and exercise much more fine-grained decisions than simple, binary choices. People may want to change specific aspects of their public exposure in response to specific changes in the environment over the course of their lifetime.[189] For example, someone may decide to take down his pictures from public view as a result of a widespread adoption of face recognition technology or because of changing a job to a one requiring more privacy (eg from barrister to judge). Finally, in respect of non-controlling, to be not manipulated individuals need to be able to rely on their decisions in the long term (eg data controllers should not reuse data for different goals without authorisation). Furthermore, as argued above, they need to control their own data because they are inherent descriptions of their personalities and identities. If data are *constitutive* for individual personalities, this makes a case for managing them in a similar manner like managing one's own body and mind. But, even if they 'merely' reflect the individuals' identities in the 'online world', the level of detail they may reveal, potential for manipulation over data subjects and risks involved justify giving them control over their own data. Also, individuals need to be able to change decisions in response to changing circumstances. This is because processes are continuous and individuals should be able to retain the ability to adapt their choices in future.

---

[188] Also, to change plans. This may be seen as corresponding to the Rawlsian conception of planning underpinning his theory of good. A person's good is determined by his or her success in carrying out the rational long-term plan of life. Rawls 1999, pp.79–80.

[189] Cf Kaye and others 2015, p.142.

Such an ability to 'correct privacy choices' may seem strange at first glance. However, as just discussed, it should be understood in light of values protected by privacy: inalienable autonomy and dignity of human beings, and, important social values. Also, it needs to be borne in mind that the scope of these considerations excludes scenarios in which public interest in personal data outbalances the individual one. So, only two interests are considered here: the interest of the individual and, usually commercial, interest of service provider. Furthermore, as it will be argued in the following chapters, some of the characteristics of the online environment are posing completely new threats and justify limitation of freedom of contract.[190] Yet, if autonomous choice is important, there should also be a capacity for individuals to make autonomous choices even if they are to their own detriment. This is not questioned. Even though individuals may agree to give up some of their privacy, there is still a case for providing them with a framework in which they would make their decisions in respect of privacy in an autonomous way, so with intention, understanding and without controlling influence.

The autonomous choice in respect of privacy process is visualised in Figure 4 below.

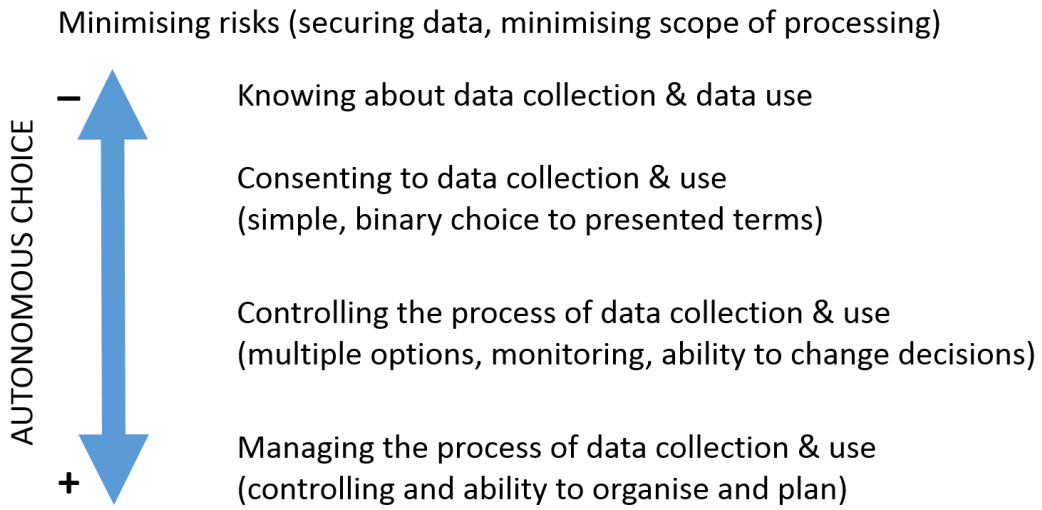


Figure 4 Varying levels of autonomous choice in respect of privacy process

As shown in Figure 4, the means for providing autonomous choice regarding the process of collection and use of personal data can be ordered with the increasing level of autonomous choice of the individual (the vertical axis). As personal data are posing risks for data subjects by their mere collection, the precondition for responsible data-processing activities is minimising those risks, excluding personal data from other data, and securing them. Also,

[190] Eg imbalance of power, information asymmetry, lack of autonomy, and externalities.

security of personal data understood as protecting them from unauthorised use is a prerequisite for any autonomous choice, because without securing the access to data others may copy them and use them for their own goals.

Then, knowing about data processing gives minimum (or zero) autonomous choice, but is a precondition for any further actions. This is because individuals are at least aware of data collection. Then, consenting to terms presented by data controllers gives a choice, but it is only a passive agreement to the presented terms. As discussed, this cannot ensure autonomy over the process. Far more autonomous choice may be provided by controlling the process of data collection and use, which presupposes that data subjects have some capacity to monitor and change or regulate specific parameters of the controlled process. As noted by Inness:[191]

> control requires both being able to regulate or even halt the progression of the situation with respect to a desired end and possessing a reasonable certainty that this ability will be retained in the future.

The important detail is that the ability to control (monitor and change decisions) is retained. As discussed, it is required as the process is dynamic. Finally, the highest level of autonomy is achieved by managing a process. This requires not only controlling, but also the ability to monitor and plan the privacy process – object of control (or management). The ability to plan represents the capacity to look forward, as described above. All of this requires such construction (or organisation) of a process of collection and use of personal data which enables individuals to make their autonomous decisions. In this view, managing the privacy process (or, in short, privacy management) may deliver the highest level of autonomous choice. It is worth noting that this description relates to managing the privacy process of an individual by an individual, while service providers are managing their own larger processes of collecting and using data of many individuals.

The concept of management is 'borrowed' from business management. In fact, it is possible to understand privacy management as a way of thinking about data processing using the methods of business management.[192] So, privacy management is the organisation and

[191] Inness 1996, p.52.

[192] Also, Betkier ("Individual Privacy Management") 2016, p.323 ff.

coordination of data activities aimed at achieving a desired level of privacy.[193] Such an approach not only leads to the use of terms which are intuitively understood, but also leads to the reuse of part of the structure of business management for data privacy. After all, business management is about managing processes, organising, monitoring and controlling resources and responding to the demands of the external environment.[194] Therefore, the functions of privacy management are similar to business management, but narrower. This thesis will present such a theoretical model (Privacy Management Model) in Chapter IV after careful examination of the commercial aspects of online services and their impact on the individuals.

D Conclusions

Data privacy is a concept which describes the sphere of individual balance between concealing and revelation of information about the self. This is becoming increasingly difficult in a world packed with data which describe individuals. Their data are gathered by service providers and used for creating profiles of individuals which are further used to influence their behaviour. Such activities are not justified by public interest, but by commercial interest in exploiting the economic value of personal data. That poses a risk to data subjects, which increases with the scope and amount of personal data and their uses. In such circumstances, the question of controlling exposure to the view of others changes to the question of controlling the streams of personal data and their uses.

The thesis adopts a non-normative account of data privacy as informational self-determination. It is a power of individuals to make their own decisions as regards the disclosure and use of their personal data. Such an account gives them more capacity to action (or, more broadly, autonomy) as to their data both in scope of what can be controlled and intensity of that control. This is important, as privacy protects the dignity and autonomy of human beings, their capacity to build social interactions, and their capacity to act as citizens in a democratic society. Understanding privacy as informational autonomy also may be reflected in the processual nature of online data activities. In such a view, privacy is a subjective, and complex process of maintaining some level of control over one's own data and their availability to others.

---

[193] Cf Robbins and others 2015, p.14.

[194] Finneran Dennedy, Fox and Finneran 2014, p.286; Robbins and others 2015, p.14.

Individuals are more interested rather in long-term effectiveness of privacy process than in making optimal choices for particular data transactions.

Informational autonomy relies on autonomous decisions made by individuals. Autonomous actions may, in particular, have a form of an autonomous choice, which may, in particular, have a form of procedure of (informed) consent. The failure of consent is related to the fact that it is inadequate for making autonomous choices in a privacy process. In this respect another tool is needed which enables individuals to take into account a full picture of their data activities, monitoring data use, and planning, making and adjusting privacy decisions in response to changing circumstances. Such a tool should be premised upon the conception of managing a process of collection and use of personal data. Privacy management is the organisation and coordination of data activities which are aimed at achieving a desired level of privacy. It requires not only controlling, but also the ability to plan and monitor the privacy process – object of management. All of this requires such construction (or organisation) of the process of collection and use of personal data which enables an individual to make autonomous decisions. This thesis will present how exactly such a privacy management model should look, but, first, there is a need to carefully examine the online services and their impact on individuals.

III What Are the Challenges from Online Services?

The formulation of a problem is a crucial first step in finding its solution. So, this chapter describes in detail online services and the way they are provided to define a privacy 'threat model'.[195] This is a systematic analysis which aims to set out the most relevant privacy problems which may be posed by online service providers. Understanding what can go wrong, and which actions of service providers breach informational autonomy, and how exactly this happens makes it possible to devise countermeasures.

This analysis is carried out in three steps. First, Part A explores and explains online businesses. It shows the role of personal data, the incentives of online companies, how they compete and create value in the market, and where those services infringe informational-self-determination. Then, Part B aims to catch the uniqueness of an 'online world' and describe why privacy problems arise there. In so doing, it explores the mechanisms which shift power in online relationships towards service providers. This is much needed to further describe both privacy problems and responses to them. Finally, Part C explains the impact of privacy problems resulting from the operation of online services on individuals and society. This impact is often neglected and, therefore, needs to be described to show the full picture of individual and social costs. Again, understanding of this impact is the vital first step in assessing the countermeasures discussed in the following chapter.

A How Do 'Data Markets' Work?

1. *Control over data is a key success factor in online markets*

What is the role of personal data in online markets? They are a central element of the modern economy and a source of power.[196] They may be used for a number of purposes, for example, delivering and tailoring services, optimising business processes, building relationships,

[195] 'Threat modelling' is also a technique for improving security of computer systems which follows a similar philosophy, eg Shostack 2014.

[196] This was understood as early as in 1970s; see Miller 1971, p.23.

reducing costs, improving risk analysis, market analysis, or targeting advertisements.[197] There is no single, unified market for personal data nor one model in which those data are used. On the contrary, there are multiple markets in which data are used as an asset for creating or increasing value from sales.[198] So, where do the personal data used in online services come from?

They come to service providers from many sources. This is because market participants cooperate to collect data from individuals.[199] Table 2 lists those sources.

Table 2 Sources of personal data available to service providers

Source	How data are collected by service providers?
Direct collection (including tracking)	Directly from individuals
Public registries	Indirectly, either from registry or by the means of data broker
Other publicly available services / websites	Usually indirectly, by the means of 'voyeur' or data broker
Third-party tracking	Indirectly, by the means of the third party
Other users	Indirectly from other users (eg tagging a friend in a picture)

Although service providers collect data directly from individuals, other sources of data are also used in the market and, therefore, need attention. Those data may come from publicly available registries, directories, electoral rolls, data related to bankruptcies, or civil judgments, all provided in the name of the public interest. Additionally, as shown in Table 2, personal data may be copied from publicly available websites (other services). As mentioned in Chapter II, there are companies ('voyeurs', data brokers) which collect personal data from all those public sources and sell them to others (including online service providers).[200] Also, data may be collected by the third parties directly from individuals by tracking their online

[197] Eg House of Lords (HL Paper 129) 2016, p.58; World Economic Forum and Bain & Company 2011, p.8; The German Monopolies Commission 2015, p.68; Spiekermann and others 2015, p.181; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, pp.23–24.

[198] Acquisti, Taylor and Wagman 2016, p.473.

[199] Ezrachi and Stucke 2016, pp.159–160.

[200] Eg Federal Trade Commission 2014, pp.iv–v.

movements[201] or physical movements.[202] Many such tracking mechanisms are designed to be invisible for consumers who do not inspect the code of, for example, websites, smartphone operating systems, or mobile apps.[203] So, to manage personal data it is necessary to address all 'data leaks' and take into account indirect data sources, and third parties processing and transferring those data.

In contrast with harmonious cooperation in collection of personal data, online services compete to capture as much consumer wealth as possible.[204] In such competition, two elements seem to be crucial: who controls (or 'owns') the end-user relationship, and who controls data.[205] First, the parties controlling the end-user relationship have a crucial ability to address users with options at the start of their 'customer journey'. This is why they are often called 'gatekeepers', because they control information "as it moves through a gate".[206] For example, this may be a Google Search used by data subjects to search for information, or Facebook's 'news feed' which is a source of news on other websites. Gatekeepers either want to decide what end users can see,[207] or want to be the first to capture their attention, for example, by the means of the starting page of their Internet browsers. Some user devices (called terminals) are to some extent configurable to enable users to set their own entry point of the Internet journey (eg PCs, smartphones). On such devices there may be a few gatekeepers, for example Google and Facebook, which is called 'multi-homing'.[208] However, there is an increasing number of terminals which not only come with a pre-set option of gatekeeper, but simply determine the

[201] By the means of mechanisms such as beacons, cookies, flash cookies, device/browser fingerprinting, tracking pixels, Acquisti, Taylor and Wagman 2016, pp.463–464; also, Neisse and others 2016, p.34.

[202] The Norwegian Data Protection Authority ("Tracking in public spaces") 2017.

[203] Hoofnagle and others 2012, p.291; Acquisti, Taylor and Wagman 2016, p.464; also, some forms of tracking (eg Wi-Fi tracking, or intelligent video analysis) are completely hidden from the data subject, The Norwegian Data Protection Authority ("Tracking in public spaces") 2017.

[204] Ezrachi and Stucke 2016, pp.159–160.

[205] Cf Page and others 2016, p.18.

[206] Barzilai-Nahon 2008; Acquisti, Taylor and Wagman 2016, p.444; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.8; The German Monopolies Commission 2015, p.58; 'gateways' in House of Lords (HL Paper 129) 2016, pp.19–20.

[207] Eg Facebook's project to deliver Internet to the developing world, Bhatia 2016.

[208] Evans and Schmalensee 2016, p.28; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.26; The German Monopolies Commission 2015, p.9.

gatekeeper without giving any choice.[209] For instance, while using smart TVs, set-top boxes, game consoles, smart cars, personal assistants, or wearables, there is usually little choice for users to change service provider.

All gatekeepers act like a hub, directing individuals (called impersonally 'traffic') to other services, and are in a position to track them across different online services, and capture data about their behaviour.[210] Other services that are not in a privileged position rely on gatekeepers, often effectively paying them to redirect customers to their content.[211] Furthermore, gatekeepers have incentives to manipulate that traffic, and influence the strategic parameters of business of parties relying on the traffic flow from gatekeepers, to make them even more reliant on gatekeepers.[212] This leads to redirecting individuals to the 'network paths' on which gatekeepers generate revenue. Not surprisingly, research finds that websites within the same advertising networks often link to each other.[213] For example, the biggest Internet firm, Google, gets redirections from approximately 78 per cent of the one million most used websites.[214]

Second, controlling vast databases of personal data is crucial to achieve and retain competitive advantage.[215] In this respect, gatekeepers are in a privileged position as they can gather more data by tracking their users. There are, however, other companies who have a huge amount of personal data, such as banks, telecoms, or online retailers.[216] Personal data are necessary for analysis to optimise and enhance online services, to gain and retain customers. Moreover,

---

[209] See the struggle to get into gatekeeper position in 'Smart TV' market, Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.21.

[210] Acquisti, Taylor and Wagman 2016, p.444; House of Lords (OPL0054) 2015, pp.1–2.

[211] Eg paying a search engine for advertising brings more traffic to a website, The German Monopolies Commission 2015, pp.58–59, note some travel websites to which 70 per cent of customers are redirected from a search engine.

[212] Hagiu and Jullien 2011, p.357.

[213] Lopatka 2017.

[214] While the next company, Facebook, gets only 32.4 per cent, Libert 2015, p.6.

[215] Ezrachi and Stucke 2016, p.238; The German Monopolies Commission 2015, p.27; World Economic Forum and Bain & Company 2011, pp.16–17.

[216] Telecoms may also be gatekeepers, however, their ability to exert control over the information flowing through their 'gates' is usually heavily restricted (secrecy of correspondence, network neutrality).

modern algorithms, such as machine learning used for many service improvements in the previous years, rely on the vast amount of data allowing them to specialise and enhance their learning processes.[217] In essence, having more and better data results in better services (because of machine learning), earning more (from better recognition of the customers), and attracting more users.[218] So, competition between service providers relies directly on the ability to "feed" their "data refineries"[219] with relevant, recent data, which may be available only for a few.[220] As a result, personal data are not only another tool of successful marketing, they are a strategic asset.

So, firms compete to design the online data market to put themselves in a position to control data flows and to gather vast amount of data, being the source of knowledge and power over the market. It is self-evident that this unveils a lot of detail about individuals. So, when do those data activities infringe informational self-determination?

2. *Which activities of service providers do pose privacy problems?*

Privacy problems may be difficult to identify and link to particular activities of service providers. They may either appear as an addition to data transactions required (or requested) by data subjects, or they may be interwoven into the fabric of online business models. The method used here for 'problem detection' is the test for informational self-determination described in the previous chapter, so checking whether data subjects are able to determine 'who knows what about them'. That is to say, whether they are likely to know who has access to their data and what happens with them. Such analysis is contextual, as people are more likely to understand that data are used in the same context as they were imparted.[221] So, to pinpoint those particular problematic activities, this section applies this method to the examples of a few typical Internet business models: 'enhanced service', trading platform, and

[217] Domingos 2015.

[218] This is caused by network effects, House of Lords (HL Paper 129) 2016, p.23 ff.; also, Ezrachi and Stucke 2016, p.145 ff.

[219] Weigend 2017, p.15.

[220] Ezrachi and Stucke 2016, p.176.

[221] Nissenbaum 2011, p.37.

non-trading platform.[222] These models are very common in the Internet, but they do not form a comprehensive taxonomy covering all possible Internet services.[223] They are a vehicle for understanding how privacy problems manifest themselves in different contexts.

(a) 'Enhanced' service model

The least intrusive model, called here 'enhanced service model', is a regular sale of products or services enabled and enhanced by using personal data, presented in Figure 5 below. It is presented here to pinpoint the activities that such service providers engage in on top of a regular sale, which impact on informational autonomy: tracking, profiling, and using 'data brokers'. They occur in all models, but they are visible here in the absence of other problems.

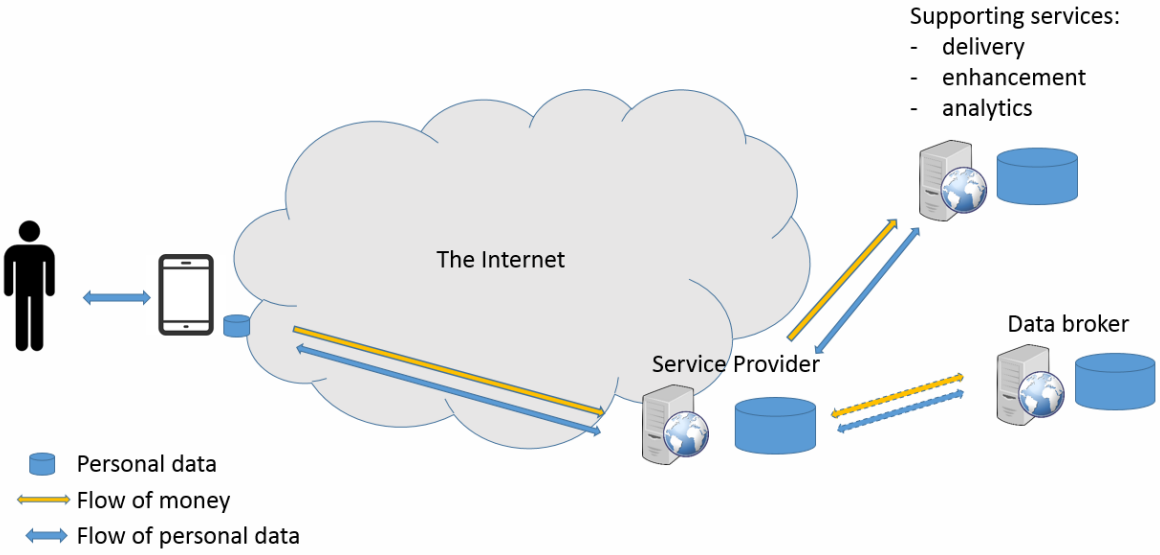


Figure 5 Enhanced service model

This model is used, for example, in e-commerce, many telecommunications services, entertainment (gaming, video, music), and some publishing.[224] In this model, there is always some monetary payment for the end product or service. This payment is based either on a transaction (eg 'pay-per-view'), or subscription (eg access to a directory of music), or on paid access to premium services while basic services are available for 'free' (so-called

[222] Those models have been well recognised by the literature, eg House of Lords (HL Paper 129) 2016; The German Monopolies Commission 2015; The Federal Trade Commission 2016. However, their selection to emphasise the privacy problems, particular elements and some names are of the author.

[223] See an approach to create such taxonomy in Page and others 2016, p.41 ff.

[224] Similarly Novotny and Spiekermann 2013, p.105, but without secondary use of personal data.

'freemium').[225] Service providers may use the supporting services of third parties (and they typically do so).

In this model, personal data are exchanged with service providers as they are necessary to provide individuals with product or service, and pay for it. They may be used for many purposes beneficial for consumers and generally desired by them,[226] for example, maintenance of the 'session' with a web server, recognition of customers so they do not need to re-enter their passwords, service customisation preserving a tailored version of the interface and customers' choices. There are also internal data uses such as gathering statistics, optimising service and detecting errors, which serve to improve service quality. Those personal data uses are predictable and probably expected. However, marketing technology uses data to provide customers with additional offers, to maintain the relationship, and to monetise data. This is the point at which profiling steps in. As a result of profiling the offers may be personalised, showing products more likely to be attractive to the customers concerned, which may be inferred from their history or from the behaviour of other users. This also may be reasonably 'benign', as long as customers are aware of that data collection and use. This is because they can decide about receiving profiled offers and decide whether they trust those service providers. It stops being benign when individuals cannot determine who knows what about them. For example, this happens when their data are collected surreptitiously, communicated to third parties, or bought from third parties for use in the requested service. As a result, web shops can know their customers as well as the owner of grocery store down the street,[227] but customers may not expect this. Such activities performed without knowledge of data subjects and giving them the opportunity to make choices are questionable and cause problems described in detail in Part C.

These problems are also caused by or/and related to tracking and data use by third parties. But, there are different types of third parties performing different roles in online services. As shown in Figure 5,[228] there are some supporting service providers (subcontractors) not directly

[225] Eg Kumar 2014.

[226] Roeber and others 2015, p.105; The German Monopolies Commission 2015, p.30; World Economic Forum and Bain & Company 2011, p.5.

[227] Eg "Intercom - Free Customer Intelligence Platform" n.d.

[228] Also in Figure 6, as these problems apply to all models.

'visible' to service users. Those subcontractors provide online firms with important services which enable them to operate (eg storage "in cloud", connectivity, payment support), to enhance the service (eg service options, like voice recognition), or to perform important but peripheral tasks, like analytics. The use of personal data by subcontractors does not infringe informational autonomy as long as they are using those data exclusively for providing the service to the end users and those end users know about collection and use of their data (attributing all actions to service providers). However, nowadays, the practice is that such third parties may collect personal data directly from the users and, sometimes, use them for their own goals.[229] In such case, service providers (eg online shops) remain the only 'visible' party for their users who may not be aware of additional third parties engaging in tracking activities.[230] So, the users cannot determine who collects and uses their data and this breaches their informational self-determination.

Another important third party is data brokers who sell additional personal data about their customers to service providers. Service providers may receive those additional data without disclosing to data brokers what they know of data subjects.[231] But, the sole fact that data brokers have huge amount of data about individuals without their knowledge nor control is questionable. In such an environment, paradoxically, individuals may be the only ones deprived of access to their own data.[232] So, in respect of data brokers, regardless of the source of their data about a data subject (eg public, observed) their actions which boil down to providing personal data to whomever pays for such access are infringing the informational self-determination of data subjects. Furthermore, as will be discussed in the following chapters, without regulating these activities any privacy management exercised in relationship with service providers would be unavailing.

---

[229] Approximately 90 per cent of top websites do that, Libert 2015; also, Roosendaal 2012; The Norwegian Data Protection Authority 2015, pp.22–23.

[230] For example, if they do not check the source code of the 'website' they visit.

[231] For example, they may match 'hash values' (cryptographic digests) of customer IDs, Federal Trade Commission 2014, p.28; Tynan 2013; 'The Data Brokers: Selling your personal information' 2014. However, note that the fact that IDs are coinciding may be recorded as additional data.

[232] Acquisti, Taylor and Wagman 2016, p.463; the notion of 'inverse privacy', Gurevich, Hudis and Wing 2014.

(b) Trading platform model

The second of the discussed business models is a trading platform. It bears all the potential privacy problems of the enhanced service model, but additionally introduces two new important characteristics which may affect informational self-determination. Those features are the aggregation of data flows by intermediaries, and decoupling the data flow from provision of the service or product. The intermediaries between user groups enabling those groups to interact economically or socially are called platforms.[233] This is commonly referred to as two- or multi-sided markets. The operation of a trading platform is shown in Figure 6 below.

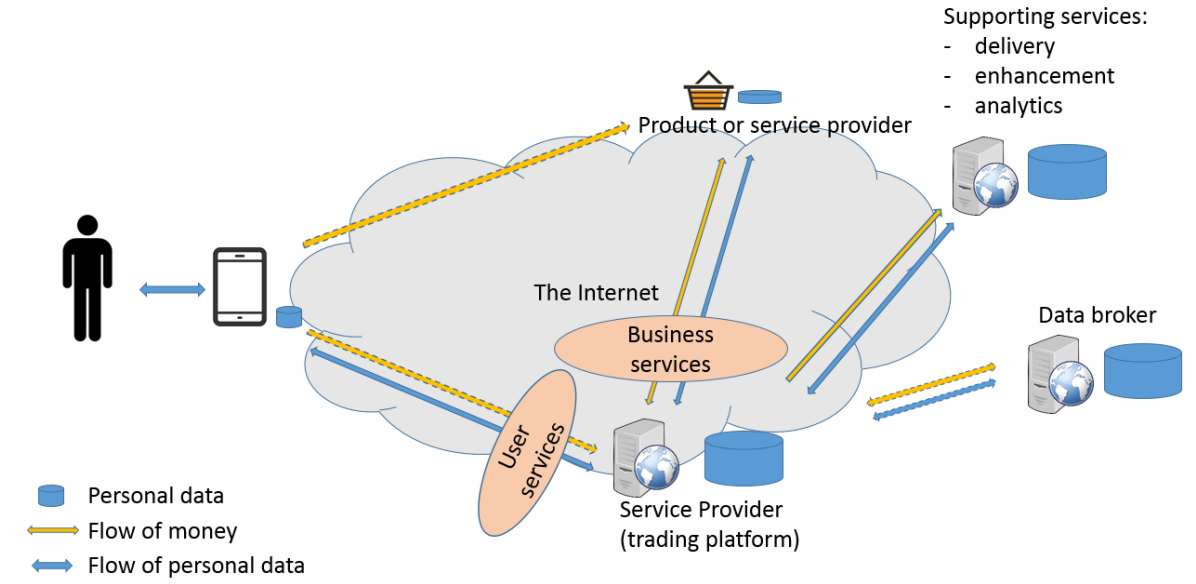


Figure 6 Flows of personal data and money in business model of trading platform

As shown above, the platform aggregates supply of end products from businesses and demand from customers. Effectively, it provides a common marketplace for those parties. This can be a model for auction platforms, like eBay or Trade Me, or the platforms of the 'sharing economy', like Uber or Airbnb. Payments for the end product may be made directly to its providers or by the means of the platform (dashed yellow lines on the left). The difference between this and the first model is that the product or service is not provided by the service provider, but by someone else. But, the customers' perception is that they are buying a product and that they exchange their personal data with trading platform *and* the end product provider

[233] The German Monopolies Commission 2015, p.19; discussion about the definition, House of Lords (HL Paper 129) 2016, pp.16–22; economic discussion should be started from Rochet and Tirole 2003 and Armstrong 2006.

to achieve this goal. So, they are (usually) aware of the existence of particular end product provider. How does this model differ from the previous one in terms of privacy?

The first difference is that a platform being a place for trade for large groups of customers may collect significant amounts of data from both sides of the market. Platforms, as discussed in the previous section, build their market position on collecting data to know the market: customers and traders. So, their business brings benefits of scale which may provide them with incentives for using data about individuals for additional marketing-related purposes. This may include selling them to business partners or even to data brokers to generate additional sources of revenue. The second difference between trading platforms and service providers offering enhanced services is that customers of trading platforms have less influence on their operations. This is because trading platforms are usually much larger, but also because the incentive of the platforms as the intermediaries is to conclude sales, but they are not liable for the end products. The details depend on the particular platform; it may provide users with some mechanisms reducing risks,[234] but, as a rule, individual customers cannot fully exercise their power as consumers towards the platforms because they are not buying from the platforms but from the end product providers. This is, however, not as problematic for privacy here as in the third model.

(c) Non-trading platform model

This is because the third model, a non-trading platform, is explicitly built on the apparent lack of connection between the user and business sides of the market. There is no product which individuals buy from businesses. User services here serve merely to attract individuals and collect their personal data to sell them on the business side. This model is implemented by all 'free' Internet services financed by advertising[235] and designed in a way in which individuals do not know what data are collected and who uses them. This schema is used, for example, by search services (like Google Search),[236] information and reference services (Google Maps),

[234] Eg The Federal Trade Commission 2016, p.33 ff.

[235] About 29 per cent of total revenue on the Internet is generated via advertising according to Page and others 2016, p.6. The payment may also have the form of commissions paid in reward for the referrals or providing so-called 'sales leads'.

[236] Cf other view, Luchetta 2012.

social networks (Facebook), some publishing, and some communication services.[237] Its details are presented in Figure 7 below.

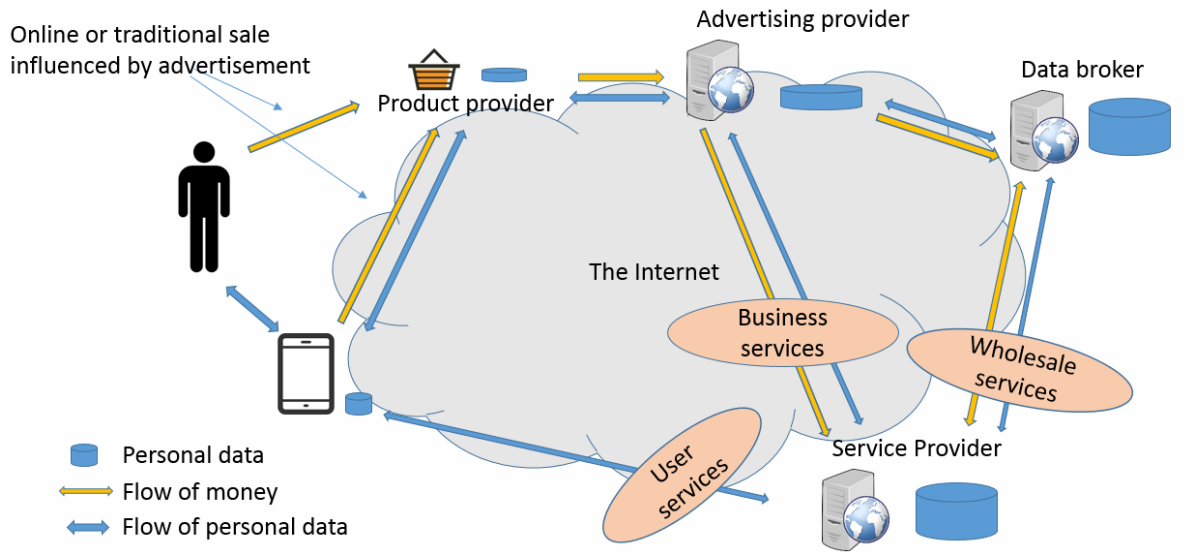


Figure 7 Flow of personal data and flow of money in non-trading platform model

As shown in Figure 7, in this model money flow is detached from data flow. Money flows to service providers from business services as remuneration for the use of personal data collected from data subjects. So, the user services of these online service providers (bottom of the picture) do not generate revenue by themselves,[238] but are cross-subsidised by the business services. However, user services generate personal data, which flow from users, and are used in a wider network of market participants[239] to generate sales revenue. That may include wholesale revenues from exchanging data with data brokers whenever it is profitable. In some hybrid variants of this model user services are only partly subsidised by advertising (eg 'freemium'), or advertising is only a generator of additional profits for the online service providers. Also, an advertising provider shown as a separate entity may be integrated by the

[237] A simplified version of the model described in The Norwegian Data Protection Authority 2015, p.10 ff. For simplicity, some elements not central to the following discussion are not shown: advertising network (websites serving ads, called also 'supply side'), ad brokers, also supporting services which have already been discussed. Similarly, Szymielewicz 1 May 2017.

[238] They may generate some revenue when, for example, those services are sold to businesses, but, this is not significant in the whole picture.

[239] Advertising may be fully automated; see the description of 'programmatic buying' or 'real-time bidding' in The Norwegian Data Protection Authority 2015, pp.13–18.

service provider.[240] But, the existence of those variants is less important at this point since they do not change the key characteristics of the model.

Those key characteristics of a non-trading platform are related to the aggregation of data and disconnection between both sides of the market (caused by the lack of the common context of engaging in the trade of a particular product or service). These characteristics are similar to those of trading platforms, but more explicit. Also, the problems they cause in this model are significantly exacerbated. Firstly, individuals have little control over online services, because they are not really their customers.[241] That is to say, they do not directly pay any money for the online services, they only 'pay' service providers with personal data. 'Paying' with personal data does not give as much leverage as paying with money. This is because personal data are collected from all individuals' actions in the digital environment, and they have no control over how much of their data is 'paid', for what, and to whom they flow. This obviously breaches their informational autonomy. And, individuals have no influence whatsoever on the monetary payment received by the service providers from advertising providers. Furthermore, some platforms are so big that consumers cannot exercise their power by boycotting them. For example, boycotting Google or Facebook (assuming that it is possible) may be seen as equal to cutting oneself off from the online world.[242] Therefore, individuals have significantly less control over the relationship with such service providers than in the first two models.

Secondly, the fact that such services are 'free' removes price competition from the user side of the market and changes the incentives of service providers towards increasing collection. This is because the primary reason for the user services to exist is not revenue generation. And, as service providers earn money from their 'real customers' on the business side, they are incentivised to increase revenue there. And, this can be done by increasing the personal data 'generation' from individuals on the user side, as the more data service providers have about individuals the better the product they have to sell.[243] But, increasing personal data

[240] For example, Google acquired in March 2008 advertising platform DoubleClick. Similarly, Facebook bought in April 2013 advertising platform Atlas. These are examples of vertical integration (see Part B).

[241] This expression was used in re:publica, Maciej Cegłowski 2017.

[242] Also, Maciej Cegłowski in Tarnoff 2017.

[243] Cf a similar, but differently accentuated view of David Evans, House of Lords ("Oral evidence from David Evans and Ariel Ezrachi") 2015, p.6.

generation exacerbates the privacy problems of individuals. They are treated as a means to an end. From this perspective, any data privacy considerations limiting data collection are an obstacle for the platforms to earn money. This is because they do not compete on price but compete on data collection.

Thirdly, an important characteristic of non-trading platforms is that the aggregation of data causes direct and indirect network effects and scale effects, which make them very powerful.[244] Direct network effects appear when online services are more attractive because they have more users. This is especially visible with the example of Facebook. They make it harder for users to switch to a different platform because people from their 'social networks' are not there. Moreover, bigger, better established service providers may have better services, because their data resources allow them to better shape their machine learning algorithms.[245] The scale and scope of data (so, volume and variety of Big Data) additionally improve the services of big service providers.[246] This means that "the strong get stronger and the weak get weaker".[247] Indirect data-driven network effects are characteristic to multi-sided markets and take place when an increase in scale on one side of the market gives additional value to the other side. This is the mechanism allowing platforms, such as Google, to offer 'free' services on the user side of the market.[248] So, while network effects seem to favour the biggest players,[249] it is harder to compete against them, and there are concerns for customer lock-in[250] and further increase of their power.[251] As a result, customers usually have little choice about personal data collection, although they might have some options provided by platforms themselves in so-called 'privacy dashboards'.[252] This, however, as will be shown in Chapter VI, is a far cry from privacy management.

---

[244] House of Lords (HL Paper 129) 2016, p.24; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.22; The German Monopolies Commission 2015, pp.19-20.

[245] Prufer and Schottmüller 2017, pp.1–2.

[246] See 'trial-and-error', 'learning-by-doing', and scope effects in Stucke and Grunes 2016, pp.170–189.

[247] Interim Synthesis and OECD 2014, p.29.

[248] The German Monopolies Commission 2015, p.20.

[249] House of Lords ("Oral evidence from David Evans and Ariel Ezrachi") 2015, p.5.

[250] More specifically, a 'behavioural lock-in' occurs when a user is 'stuck' in some inefficiency due to habit, organisational learning, or culture, Barnes, Gartland and Stack 2004, p.372; also, Kim 2013, pp.79–81.

[251] Conseil National du Numerique 2014, p.5.

[252] More in Chapter VI.

So, looking at the examples of business models in this section it is possible to discern activities which create privacy problems. Those activities which appear independent of the business model are tracking, profiling, and the use of data brokers. In the course of all of these activities individuals are not able to ascertain who knows what about them. Additionally, the more data are aggregated and the less connection between services on the user and business sides of the market, the greater the potential to infringe on informational autonomy. This is because individuals have less influence on service providers and less information about what data are collected and how they are used. Information autonomy seems to reach its minimum in the non-trading platform model, where personal data are the only 'goods' exchanged between the two sides of the market.

All these findings will be addressed later in this thesis. But, first, it is necessary to answer the question: where does the economic value of data come from?

3. *Economic value of data*

The questions: 'where is the money?' and 'how much are data worth?' are crucial for any discussion about the market and, more broadly, for understanding the issues under discussion in this thesis. As discussed above, the economic value of personal data can be derived from enabling or enhancing transactions.[253] In all models discussed in the previous section profiling individuals has the same aim: to describe them by means of their data as well as possible. In 'enhanced services' and 'trading platform' models personal data are mainly used to enable and enhance transactions the individuals know about with firms which are also known to them. Therefore, as long as service providers do not use data for other purposes, both parties may benefit from the additional economic value of personal data exchange. However, in the 'non-trading platform' model service providers sell to their customers (ie advertisers) the promise of access to data subjects.[254] This is the point at which the economic value of data in this model is created. It is a present value of the money which may be earned (or saved) by using personal

[253] Eg OECD (DSTI/ICCP/IE/REG(2011)2) 2013, p.16.

[254] Whittington and Hoofnagle 2012, p.1350.

data to influence the data subject in future.[255] This influence, if successful,[256] usually leads to concluding a contract with the individual (an advertisement-led sale) in which the data subject pays for the end-product together with profiling activities targeted against them. A very similar mechanism operates in scenarios which are on the surface 'non-commercial', so do not lead to concluding a contract with individuals. For example, political parties may pay from received tax or donation money[257] to influence the group of individuals to vote for them, based, for example, on their psychographic profiles.[258] In all those scenarios in non-trading platform model the economic value comes from the ability to influence (or manipulate) data subjects, therefore from affecting the personal values of privacy. From the perspective of the data subject, this is monetised at the moment of paying for the end-product.[259] From the perspective of non-trading platform, the monetisation comes from earning wholesale payments from advertisers (based on number of ad impressions, sales commission, or other). So, how can those data be valued?

One way of looking at the economic value of data is to see them as having monetary value. At the moment that personal data are collected their future value is uncertain,[260] but it is already possible to make some estimation based on current incomes of service providers for similar data.[261] This is the way the value of data is described in so-called 3V model of 'Big Data'.[262] This model emphasises that the value of data comes from their volume, variety of sources, and velocity of their accumulation and use.[263] The value of data is higher if data subjects' profiles are more complete. This is because they may be matched more accurately by computer

[255] Cf Acquisti, Taylor and Wagman 2016, p.444.

[256] Successful for service provider. Success for data subjects should be defined differently.

[257] Depends on the system of financing of political parties.

[258] For example, targeting highly neurotic people with fear-based ads. See how this can be 'sold' in Concordia 2016.

[259] Or, paying taxes to government for their advertisements.

[260] Because it is not known yet whether and to whom they will be sold.

[261] Cf Mayer-Schönberger and Cukier 2013, pp.120–121.

[262] More in Federal Trade Commission 2016, pp.1–2; also, D'Acquisto and others (ENISA) 2015, pp.10–11.

[263] Cf versions with 4V (additionally value) or 5V (additionally veracity).

algorithms to the 'look-alike' profile, so to the profile of the desired customer.[264] In these circumstances individuals can be presented with an offer which is more likely to succeed (as being better 'tailored' to them). How much are personal data used for such offer worth?

There are studies which aim to assess the monetary value of data. For example, Olejnik and others found that average advertisement was traded at US$0.0005.[265] This may explain the number of advertisements individuals receive. A more complete picture gives the ARPU (Average Revenue Per User) of big online service providers. For example, for Q3'2017 Facebook had worldwide ARPU from advertising of US$4.97, while in the US and Canada it was US$20.69.[266] Google's quarterly ARPU two years earlier (in 2014) was US$45.[267] These amounts show how much money those providers receive from a statistical data subject. Interestingly, they are smaller or similar to the amounts people are willing to pay for a service which is privacy protective.[268] But, there is no option with Google or Facebook to have a paid, but privacy protective service. Also, many people are willing to sell their personal data. For example, the Boston Consulting Group study presents such willingness to provide to organisations different types of data in response to some indicative price:[269]

[264] Data of the targeted person are compared to data of the ideal customer, for example the one who already bought the end product or service, Zawadziński 15 February 2017; Szymielewicz 1 May 2017; also, Hayter 6 September 2013.

[265] Olejnik, Minh-Dung and Castelluccia 2013, p.13; see the review of such studies in Acquisti, Taylor and Wagman 2016, p.478.

[266] Facebook ("2017 Q3 Results") 2017, p.8.

[267] Google stopped reporting ARPU after rearranging its capital group in 2015. The last report is presented in Garner 11 Febuary 2015.

[268] Acquisti, Taylor and Wagman 2016, p.478.

[269] The Boston Consulting Group 2012, p.34.

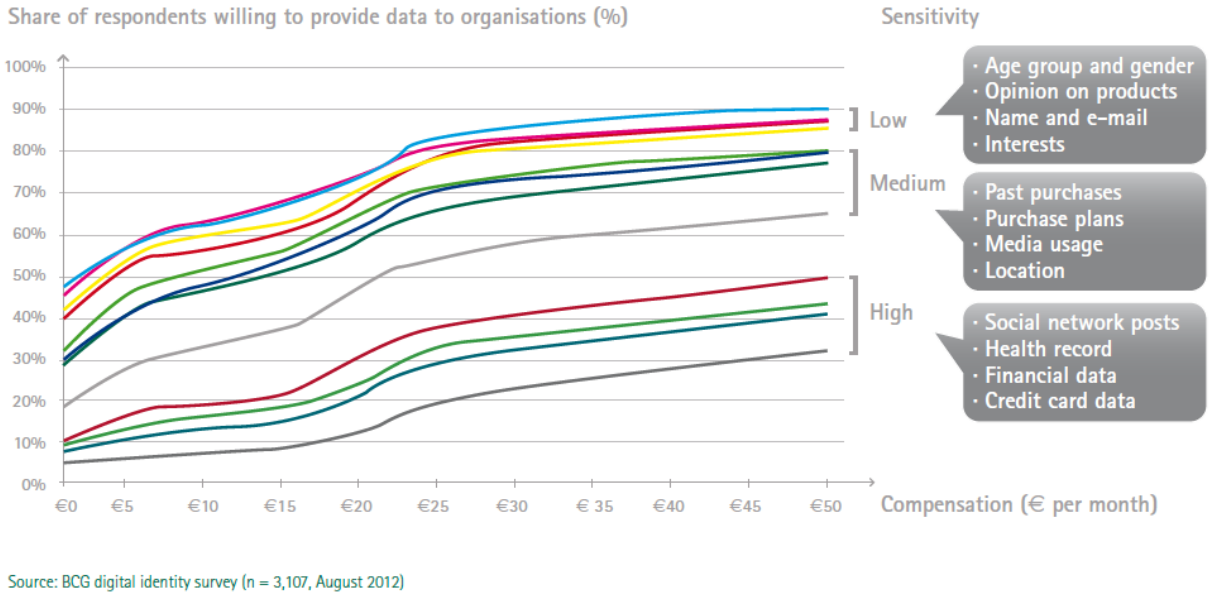


Figure 8 Respondents' willingness to provide their personal data to organisations as a function of monthly compensation

Looking at Figure 8 above, it is possible to conclude that first, the economic value people place on data depends on the type of data and, second, that is to some extent measurable and tradeable. But, the prices people expect for their data are often higher than what service providers earn on them from their customers. This suggests that data subjects do not give their data as a result of an equal bargain.

Another way of looking at the economic value of data, is to consider data as actually being a personal currency for online transactions.[270] This conceptual exercise is worth doing because such commodification of personal data exposes deeper problems. As with other currencies, personal data are exchanged for goods and services, and store value. It may be said that individuals pay with their data for services. Such a method of payment may be considered convenient as there is no requirement to pay before service delivery. It also allows literally anybody to access and use (some part of) online services, regardless of their financial capacity.[271] Similarly, Interim Synthesis in a report for OECD claims that data as "shared

[270] Eggers, Hamill and Ali 24 July 2014; The German Monopolies Commission 2015, p.27; Interim Synthesis and OECD 2014, p.22; House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.11.

[271] The quality of such services is, however, comparable to the quality of television paid by advertising – only good enough to cause the audience to view advertisements.

means to many ends" are an infrastructural resource, a capital good.[272] In fact, companies treat data as capital (capital goods or financial capital). They accrue personal data and build competitive advantage on excluding others from using their resources.[273]

Although conceptualising data as a currency or a capital generating money may be thought to devalue privacy concerns related to personal value,[274] it exposes the problem of lack of control over such currency. Usually the use of currency or capital can be controlled by its owner, which is not true in the case of personal data. Although data controllers have control over personal data in their ICT systems, data subjects have very little. They do not know how much they really pay for online services.[275] In fact, the price of online services (in data) is not defined and, as a result, each user pays their own price depending on their individual consumption pattern. If one assumes that data are a currency and imagine them as cash, it becomes clearly visible that data subjects have 'holey' wallets (because of third party tracking), no control over their spending, and very little access to their 'bank accounts' – collections of their data in the ICT systems of service providers. And, as a result, this parallel between personal data and money gives some guidance to the steps to secure data subjects' 'wallets' and 'accounts'.[276]

Knowing how data markets operate, it is possible to identify common characteristics of the online environment (Part B), and describe problems generated by services in that environment (Part C).

B What Makes 'Cyber' Special?

All this leads to the questions: Why is 'cyber' different from 'real'? Why does the online environment pose those problems for individuals seeking to ascertain who knows what about them?

---

[272] Interim Synthesis and OECD 2014, pp.22–27. They argue, however, that personal data cannot be considered as a currency.

[273] House of Lords (OPL0046) 2015, p.4.

[274] See Part C.

[275] House of Lords ("Oral evidence from Daniel Zimmer and Thomas Weck") 2015, p.16.

[276] See the next chapter.

There are well known generic features of the online environment relating to its technological characteristics which have an impact on privacy. That is to say, as presented in Chapter II, the use of ICT generates and accumulates enormous amounts of personal data describing individuals.[277] Those data can be made available instantly, anywhere, anytime, by anyone. They can be sent to any part of the globe over the computer networks at virtually no cost.[278] Additionally, they are much more accessible in terms of ease of searching through the world-wide 'Internet archive'. What is not closed behind the walled gardens of a particular service provider (like Facebook) or protected by cryptography, is scrutinised by so-called search engine crawlers[279] and potentially available for searching. Furthermore, most online service providers keep those data for an indefinite period, so in practice forever. All of this is important, but reasonably well known. This Part will focus on a less widely understood aspect of the online ICT environment – the influence of technology on the relationship between data subjects and service providers. This relationship is mediated by computer systems,[280] which has several important consequences.

1. *The architecture of online environment*

The first consequence of mediation of the relationship between data subjects and service providers by computer systems is that the field of interaction, ie the architecture of online services, is fully determined by the service providers.[281] From a user's perspective, those services are usually seen as pre-designed documents and forms organised in a linked structure permitting users to navigate between those documents and exercise pre-defined operations. This pertains not only to websites, but essentially to all modern graphics-based applications (eg mobile 'apps'). They are designed and controlled by service providers who determine which user actions are possible and which not. Many authors note that online architecture imposes constraints on users, but is also much more flexible than architecture of the physical

[277] Korff and Brown 2010, pp.12–14.

[278] There are, of course, costs of building and using networks. The perception of free access and use of the Internet is a result of the prevalent retail pricing schemas which are not based on transfer.

[279] There is an option to signal opt-out from such access.

[280] Calo 2014, p.1004.

[281] Betkier ("Individual Privacy Management") 2016, p.317.

world.[282] In the online architecture, service providers create the process of interaction between individuals and service by designing a so-called 'customer journey'.[283] In those processes customers may only 'travel' along a pre-designed path. Even if this path depends on some options, those rely heavily on default settings pre-set by service providers.[284] In this interaction users may also be to some extent supported by their computers and additional software. For example, users may install software, such as the web browser plug-in 'Disconnect',[285] which prevents some tracking activities or, at least, makes them overt. However, those actions have, in general, limited impact. This is because a limited knowledge about such tools exists, and because of the problem of vertical integration.

Vertical integration is a wider problem as it reinforces the market power of service providers by eliminating competition from the value chain[286] of online services. Figure 9[287] shows a value chain in which steps adding value to online services are ordered from production (left) to consumption (right) along the horizontal[288] axis.[289]

[282] See 'the code', Lessig 2000; earlier ideas in Reidenberg 1998; extension to hardware and network protocols, Greenleaf 1998; also, Giblin 2011, p.8.

[283] Richardson 2010.

[284] This was empirically verified, Tschersich 2015; detailed description of this mechanism, Thaler and Sunstein 2009.

[285] 'Disconnect' n.d.

[286] Value chain analysis is one of the tools of strategic management analysis introduced by Michael Porter in the 1980s. When used to present the whole industry it shows which market players and in which order introduce value in the process of production in a given market – between the creation/production of the product components and consumption by the user.

[287] Originally used in Moreham and Betkier 2016, p.23.

[288] The axis is horizontal for practical reasons; the notion of 'vertical integration' comes from the analogy to a river and understanding markets as being 'upstream' or 'downstream'.

[289] On the base of Page and others 2010, p.6; also, Page and others 2016, p.12.

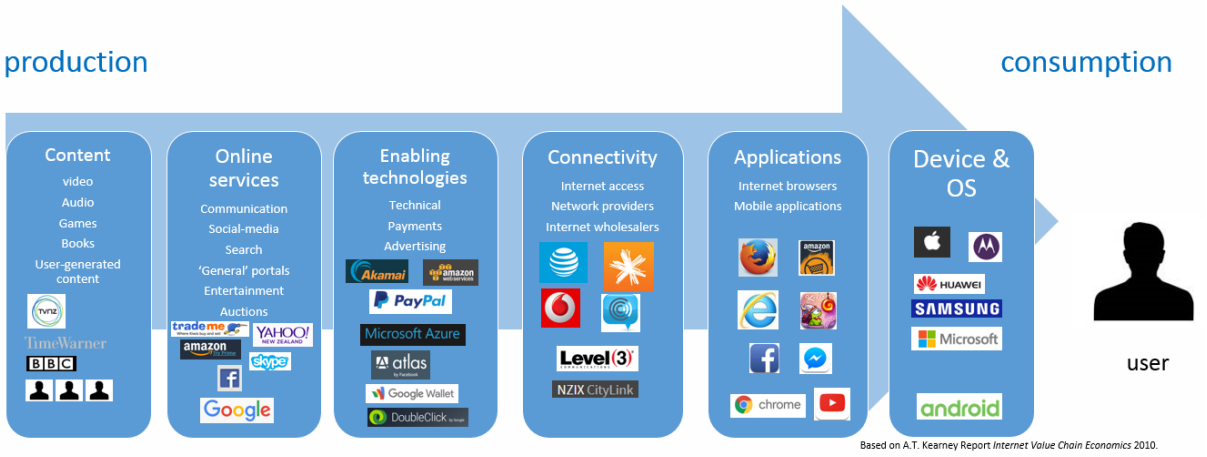


Figure 9 The value chain of Internet services

As shown in the picture, the same companies and their subsidiaries are present in most of the links from left to right. For example, Google provides online services (eg Google Search, Gmail, Maps), enabling services (eg Google Cloud for storage, Google Wallet for payments, DoubleClick for serving advertisements), delivered to users via Google applications (eg Chrome for search, Google Maps for navigation, YouTube for video) in Google's operating system (Android) which may even be running on a Google-provided smartphone (Pixel). Furthermore, Google and Facebook have plans to provide Internet access globally,[290] which will effect further integration of the chain 'link' indicated in the picture as 'connectivity' (occupied by telecom operators). The point is that in such an environment the biggest service providers use their power on some markets (so, the competitive advantage arising from using data) to reinforce their positions on markets upstream (supplying) or downstream (buying) to them. As a result of such integration, there is less competition and less choice of service provider for data subjects.

Vertical integration extends data surveillance to user terminals with the effect of turning them into 'electronic leashes' which identify and track online and physical movements of data subjects. For example, mobile apps can track users' movements more accurately and with fewer restrictions compared with the same services available in web browsers. Furthermore, there is a trend to force customers to log into online services or even into their own devices.[291] This identifies them for the purposes of secure access to the service, but also for data

[290] Google's project, "Loon for all – Project Loon" n.d.; Facebook plans, Hempel 2016.

[291] Eg using Apple ID is mandatory, while avoiding using a Google Account or Microsoft Account is cumbersome, see Betkier ("Individual Privacy Management") 2016, p.318.

collection. As a result, the users have lost the ability to understand and control their own devices[292] and are denied the (possible) advantage of using their own mediating software. Also, automatic updates frequently change the software on those devices, altering the way they work, often without users' knowledge.

Furthermore, only a few of the biggest online service providers have the ability to provide a wide range of 'free' services to which users subscribe and remain 'locked in'.[293] For example, it is hard to resign from Facebook because it is a platform for communication with many friends, communities, and even government authorities. Similarly, it is hard to replace a 'free' mailbox provided by Google with virtually unlimited disk space together with a set of office tools (Google Docs) with a set of particular, non-integrated tools. Also, those service providers are able to provide security for the personal data of their customers.[294] So, individuals need to find protection by those service providers for reasons of security and convenience. This is why Schneier describes the relationship between them and their users as feudal.[295] Once users subscribe to the environment of those 'feudal lords', they must surrender their personal data.

The last important fact related to the architecture of online services is that they are usually centralised. That is to say, most of them (eg Google, Facebook, Amazon, iTunes) are built in the 'hub and spoke' model in which individuals gain access to one central 'service place'.[296] And, as noted above in Part A, they compete with their personal databases by excluding them from open access and selling personal data piece by piece as wholesale 'products'. This, surprisingly, is good news for data privacy as those personal data which have value for service providers are already excluded from public access, to some extent secured,[297] and available in their 'hub and spoke' environments which may bear some resemblance to 'bank accounts'. So, the problem is not that the personal data are not protected at all, but that the interests of

[292] Furthermore, they are turned to gather data about other users through, eg contact books on smartphones, tools for tagging friends on social media and face recognition technology.

[293] Pariser 2011, p.40.

[294] Ie security from others, not from them.

[295] Schneier 2013, p.16.

[296] Despite the fact that these services may be built from distributed components, they appear to their users as one central service.

[297] To the extent which protects data controllers against the adverse consequences of data loss, London Economics 2010, p.xvi.

the individuals have not been taken into account in data-processing activities. It is the service providers' interests which prevail.

2. *Information asymmetry and individualisation*

The second consequence of computer-mediated communications is that they create asymmetry in information and knowledge, which disadvantages individual users.[298] That is to say, service providers use data to create knowledge about data subjects, who do not really have the information or tools to ascertain what service providers do. There are several reasons for this disadvantage. First, service providers control their architecture as discussed above. Furthermore, as ICT technology is relatively new, social rules governing their use are elastic.[299] This malleability enables service providers to design their architecture to optimise 'sharing'. For example, Facebook default settings over time slowly changed towards public exposure of personal details.[300] Second, data collection is usually hidden, and transactions on the other side of the market are not visible to data users.[301] They may not simply be aware of the fact that their data are continuously aggregated and each additional piece is refining their profiles.[302] Third, individuals lack computer knowledge. They may not realise that the hyperlinks which take them from one website to another are usually created by advertising software.[303] As the online environment is relatively new, they may use analogies with the real world, which may be misleading.[304] For example, they may think that service providers have only the access to the same functions of the service as individuals (thinking that real objects look the same regardless of observers). Or, that the communications sent to individuals on the Internet are the same as communications to others (analogy to traditional media which broadcast the same messages to groups of people). Both of these analogies are misleading. Communication in the online environment is not only mediated by computer, but also

---

[298] Betkier ("Individual Privacy Management") 2016, p.319.

[299] Ibid., p.320.

[300] McKeon n.d.

[301] Eg 'iceberg model', Debatin, Lovejoy, Horn and Hughes 2009, p.88.

[302] Whittington and Hoofnagle 2012, p.1327.

[303] Lopatka 2017.

[304] Betkier ("Individual Privacy Management"), p.321.

individualised to a particular user profile, and may be manipulative.[305] As a result, uninformed individuals 'share' more and do not use available methods of control over data collection.

Information asymmetry may be one of the main reasons for the dichotomy between declared privacy-protective attitudes and the evidence of privacy-careless behaviours.[306] Conscious, well-informed customers would not disclose too much information to the other side of transaction because it might create an incentive to discriminate against them.[307] Yet, this is exactly what people do online, giving away their personal data which end up in the possession of the other side of transaction. But, this dichotomy may be also caused by contextual cues to which individuals respond more strongly with providing their data than to objective risks and benefits of doing so.[308] Or, they may be lured by the promise of the immediate gratification (from using the service or from other users via 'likes') which distorts rational decision making for both naïve and sophisticated individuals.[309] Also, the decision to give consent for data processing and to enter into contract is one-off, while such a contract is a long-term one with multiple privacy risks that are very hard to assess and control.[310] For individuals, it may be not possible to monitor the execution of such a contract as there is currently no possibility to check how online providers use personal data. All of these arguments together with conclusions drawn in Chapter II about the problems of consent suggest that information asymmetry problem may not be solved only by giving individuals more information before obtaining their online consent. The problems are inherent in the system, which itself needs to change if individuals are to be given meaningful control over their data.

Furthermore, in the online environment data subjects may be thoroughly described and individualised by data holders. This was not the case in the early Internet era which was underpinned by ideas of enabling individuals to have access to information, so they could learn and benefit.[311] Such an approach was linked to anonymity of users. This, however, changed in

[305] Eg experiment on Facebook users, Kramer, Guillory and Hancock 2014.

[306] Acquisti, Taylor and Wagman 2016, p.477.

[307] Brown 2013, p.2.

[308] John, Acquisti and Loewenstein 2011.

[309] Acquisti 2004, p.27.

[310] Whittington and Hoofnagle 2012.

[311] Pariser 2011, pp.102–104; also, Berners-Lee 1989.

the process of commercialisation of the Internet. Access to shared information was complemented and substituted by individualised communication targeted at specific people. This is because the Internet is a platform which gives the promise of solving the inefficiency of advertising. This inefficiency was explained in the old adage that half the money spent on advertising is wasted, but there is no way to find out which half.[312] The businesses attempted to remedy this problem by tracking Internet users and completing their profiles, in other words, not only identifying them, but also individualising them by creating profiles based on personal data. According to some authors this goes as far as creating complete a digital replica of individuals, which is feasible in the world of Big Data.[313] Others say that the service providers' business is, in fact, to know and monetise what is on individuals' minds.[314] This may seem far-fetched, but there are real projects aiming to do exactly this.[315] This changed the Internet. Although many may believe that they are anonymous while using the Internet, this is no longer true.

So, the commercial part of the Internet is no longer as much about discovery and access to knowledge, but about creating a virtual picture of its users and shaping their environment according to that picture. Pariser called this phenomenon 'the filter bubble'.[316] The content people see on the web often depends on their profiles and commercial goals of service providers. The offers they receive may not be the 'standard offers' they know from 'brick and mortar' shops, but are 'tailored' to their profiles. The prices for goods, services, financial transactions, and so on, may be 'individualised' as well. As a result, data subjects are individualised, fully 'visible', and transparent to service providers and, therefore, exposed for their actions.

Importantly though, in spite of such individualisation, communication between the parties does not get personal. There is no direct personal communication between the parties in a computer-mediated architecture. This is of utmost importance for consent and distinguishes

---

[312] Attributed to John Wanamaker.

[313] Iyer, Subramaniam and Rangan 2017.

[314] Pariser 2011, pp.102–104; cf privacy as right to own mind(space), Turkle 2015, p.303; also, Edward Snowden's definition of privacy, "A Conversation on Privacy" Chomsky and others 25 March 2016.

[315] Statt 2017; see Solon 19 April 2017.

[316] Pariser 2011.

its role in this arena from the role it plays in, say, medical law. 'Medical' consent has a chance to be 'informed' due to personal communication with an expert (doctor) who may explain the risks of a medical procedure in language adjusted to the capabilities of particular patient. In the computer world, all users see the same T&Cs and adhere to them either by clicking on a pre-fabricated form, or just by using the service functionality. Despite information asymmetry, there is no expert advice before entering the contract. Furthermore, there may be no personal communication at all between service providers and their users.

So, the online environment creates a great asymmetry of information to the disadvantage of individuals. The power of service providers is based on controlling the architecture designed to incentivise individuals to leave as many data as possible. Individuals' weakness is a combination of factors including lack of awareness, expertise and vulnerability to cognitive biases. Furthermore, there is also a systemic dissonance between the nature of the long-term contract with multiple risks currently not able to be controlled by the individual, and the expectation of making one-off consent decisions. All of this suggests that information asymmetry cannot be solved by simply providing individuals with more information before concluding online contracts. As this thesis will show, other options need to be considered.

C Privacy Problems in Respect of Online Services

So, what privacy problems do result from the actions of service providers and the characteristics of the online environment described in the previous Parts? There might seem to be little harm in collecting mundane data about daily activities, for example about interactions with friends on Facebook or search phrases. Also, individuals may perceive giving out personal data as a small price for those services. Where is the detriment flowing from such activities?

As outlined above, the detriment for the individual is usually compound, and, similar to privacy values, has three dimensions: risk of tangible (usually economic) loss, impediment to

dignity and autonomy, and detriment to social values. They are described below in this order.[317]

1. *Risk of tangible loss to the individual*

To better understand the risk of tangible loss caused by personal data processing, it is useful to express it in the language of risk management. In this view, personal data processing poses a hazard (potential source of danger)[318] to data subjects and the scope and extent of data activities increases the risk of the occurrence of adverse consequences.[319] This risk emerges at the moment collection starts and increases when more data are collected, revealed to more parties, combined with other data, and reused in different contexts.[320] This was explained in Figure 3 in Chapter II. Although some service providers introduce advertising policies to prevent some consequences,[321] the nub of the problem is that the very point of the activities described in Part A is to influence individuals, so the risk is systemic and cannot be removed.[322] The adverse consequences are usually economic and rely on using information about data subjects to their detriment: using data to discriminate against data subjects, manipulating or expressly coercing them to do things they do not have the will to do, or using of someone's identity data to commit a fraud ('identity theft'). Each will be considered in turn.

First, discrimination relies on the ability to use data to individualise offers and select people to whom they are presented, but also on individualising the way contracts are executed. These are to some extent normal business activities (for example, targeting offers to people who may be interested in taking them), but may also be based on factors considered discriminatory (eg

[317] Cf other approaches to describe privacy problems. In the order of data processing activities, Solove 2006; along subjective-objective division, Calo 2011, pp.13–14; based on data controller's activities, Korff and Brown 2010; based on data subject's activities, Grimmelmann 2009.

[318] Definition in Oxford English Dictionaries.

[319] But, the eventuation of the risk (ie the consequences) may be postponed or may not happen at all, Fischer-Hübner and others 2013, p.3.

[320] Eg D'Acquisto and others (ENISA) 2015, pp.12–14.

[321] Eg Facebook ("Advertising policies"); Google ("Advertising Policies Help"); they prohibit some content and practices of advertisers.

[322] Eg Mark Zuckerberg says "there will always be bad actors", Levin 21 September 2017.

race, sex, religion, sometimes income). Such discrimination may take place, for example, in employment processes,[323] in a subsequent employment contract as a result of 'workforce analytics',[324] by presenting different prices for the same products to different viewers,[325] or by not presenting some products or elements of products to selected viewers.[326] Furthermore, in the world of 'Big Data', discrimination is possible even without referring directly to discrimination factors.[327] This is because data may reflect (and perpetuate) the effect of existing inequalities (eg people of a particular skin colour may already be poorer or live in a particular neighbourhood). Such behaviour may be not intentional, but Big Data also give the ability to disguise intentional discrimination as accidental,[328] and hide it behind the cloak of mathematical equations.[329]

Second, manipulation occurs when data controllers covertly pursue their economic interests over the interests of data subject. Probably the most offensive type of manipulation is exploiting the vulnerabilities of the weak – the poor, old, or uneducated. Such behaviour was identified when data brokers were selling the so-called 'sucker lists' compiled of consumer with particular bias or vulnerability simply to the highest bidder.[330] Targeting youth with advertisements related to unhealthy food bears similar characteristics.[331] Non-economic consequences may also occur when an individual is manipulated into activities or into supporting particular ideas. For example, some data analytic companies use data to *change behaviour* of people (market behaviour and political behaviour).[332]

Furthermore, coercion is an overt use of controlling influence which may be gained by analysing data. The strongest form of coercion is blackmail, where someone threatens to

[323] Acquisti and Fong 2014.

[324] Kim 2017.

[325] Based eg on their browsing or purchase history, Hannak and others 2014, p.317.

[326] Mikians and others 29 October 2012; also broader in Gutwirth and Hildebrandt 2010, p.34; Schermer 2011, p.47.

[327] Korff and Brown 2013, pp.18–29; Barocas and Selbst 2016, p.691.

[328] Barocas and Selbst 2016, pp.692–693.

[329] O'Neil 2015.

[330] Angwin 2015, p.17; Calo 2014, p.1015.

[331] Schwartz and Solove 2011, pp.46–49.

[332] "Cambridge Analytica" n.d.; See also sales presentation of election influence Concordia 2016.

expose secrets learned from personal data if the individual does not accede to demands.[333] However, coercion may be also disguised in the consent form with Terms and Conditions. For example, what can the user do if access to the system containing important data is locked down and the request to read and agree to change of T&C is displayed? It is not a free choice when the user has no other practical option than to click 'I agree'. Coercion may also take place when an online entrepreneur uses the advantage of information to raise prices. For example, it may happen that a flower shop knows that this particular customer is willing to pay more (because of reconciling with their spouse, birthday of fiancé, child birth, funeral, etc.),[334] or, in the taxi which raises prices in response to demand – on Valentine's Day or even during a terrorist attack.[335]

The third potential adverse consequence of data processing, 'identity theft' is one of the most common online frauds.[336] According to the OECD report about identity theft people's identity is typically used for: misuse of existing 'accounts' (eg bank accounts),[337] opening new ones, fraudulently obtaining government benefits, services, or documents, health care frauds, and the unauthorised brokering of personal data.[338] The importance of this problem is increasing, although the statistics about the impact are divergent[339] and exact numbers, especially those derived from surveys, may be far from accurate.[340] Those activities are obviously criminal, and will probably be a growing problem because of the growing importance of the 'digital economy'[341] in which people are represented by their data.

---

[333] For example, the leak of sensitive data from 'adultery portal' Ashley Madison created a wave of blackmail, Zorz 2017; more about the leak in "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner - Office of the Australian Information Commissioner (OAIC)" n.d.

[334] Based on Calo 2014, p.1024; Simpson 2014.

[335] Simpson 2014.

[336] Eg according to British report in 2016 it was reported 173,000 in the UK which makes 53 per cent of all frauds, CIFAS 2017, p.7; also, estimated 8.5 per cent of Australians affected by misuse of their personal information, Attorney-General's Department, Commonwealth of Australia 2016, p.5.

[337] Eg Popper 21 August 2017.

[338] OECD 2009, p.9.

[339] OECD 2009, pp.33–41.

[340] Florencio and Herley 2011.

[341] Eg The Boston Consulting Group 2012, p.9.

But, what is characteristic to privacy economics is that all the above consequences pertain mainly to data subjects. In the language of economics this phenomenon is called 'negative externalities'.[342] They exist when some activities of a producer impose costs on third parties (here, data subjects and society) that are not reflected (internalised) in the price of the product.[343] In respect of personal data, negative externality occurs when an economic decision of data controllers, for example, to sell data to third parties, creates costs for individuals.[344] In the case of online services, a data controller does not usually bear any significant negative costs of the misuse of data[345] or may even have the incentive to sell personal data for marketing. The negative consequences are suffered predominantly by customers as they may, for example, experience identity fraud.[346] Similarly, Schneier notes that for the same reason companies do not have the incentive to improve data security.[347] Again, all this is important to understand the context in which consent or any alternative system for individual authorisation will be operating. The thesis will address these issues in the following chapters.

2. *Harm to individual values – autonomy and dignity*

Although the language of risk may be helpful to describe the economic dimension of privacy harm, it is not capable of addressing fully other values protected by privacy. This is because dignity or autonomy losses are not (only) risks of future adverse consequences. They have an immediate impact on individuals. This impact occurs by diminishing the capacity to act autonomously (towards individual goals). It may be sometimes subtle, but is pervasive, constant and usually related to adverse consequences discussed in the previous section.

Mass-scale data collection is usually described in terms of 'surveillance'. The relationship between online service providers and data subjects can be compared to the Panopticon model,

---

[342] Wider perspective in Trebilcock 1993, pp.58–60.

[343] Eg Ogus 2004, p.35.

[344] Acquisti, Taylor and Wagman 2016, p.452.

[345] For example, stock price in result of publishing information about data breach changes only 0.6 per cent for the next day and this change is practically eliminated within a few days, Acquisti, Friedman and Telang 2006, p.12.

[346] Brown 2013, p.5.

[347] Schneier 2015, p.193.

the concept of surveillance created by Bentham and developed by Foucault.[348] As in the panoptical prison, data subjects are individualised and constantly visible, but deprived of the capacity to check how their data are used. The architecture of online services and asymmetrical view work exactly the way predicted by Foucault. That is to say, it is a disciplinary mechanism incorporated in an economically efficient, architectural structure exercising power over individuals.[349] Individuals do not see the power, but they are regulated on a continuous, pervasive, and highly granular basis.[350] As a result, the free environment which can stimulate and can be discovered by the individuals is substituted with an environment which is controlled by commercial algorithms and 'pushes' individuals into actions beneficial for service providers.[351]

There are also other, perhaps more sophisticated models of surveillance.[352] For example, Haggerty and Ericson use the term 'surveillant assemblage', which operates by "abstracting human bodies from their territorial settings and separating them into a series of discrete flows", which are then "reassembled into 'data doubles' which can be scrutinised and targeted".[353] In their view, the surveillance is no longer hierarchical and originated from a central point, but "rhizomatic", without centre.[354] Also worth noting is the concept of 'surveillance capitalism' by Zuboff, which "thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behaviour".[355] She concentrated on online service providers who, in her view, offer in the markets of behavioural control rights to intervene in an information loop of data subjects' devices and, indirectly, data subjects.[356]

All these models show the infringement of individual values by those engaging in surveillance of users' online activities. First, they point to modification of the behaviour of individuals

---

[348] Betkier ("Indvidual Privacy Management") 2016, p.322; Foucault 1995, p.200. Foucault built his conceptions on the basis of the work of Nikolaus Julius.

[349] Foucault 1995, p.219.

[350] Yeung 2017, p.131.

[351] Cohen 11 March 2015.

[352] Galič, Timan and Koops 2017; also, Marx 2016, p.291 ff.

[353] Haggerty and Ericson 2000, p.606.

[354] Ibid., p.617.

[355] Zuboff 2015, p.85.

[356] Ibid., pp.85–86.

against their wishes, so the infringement of their autonomy. Persons who are disciplined, regulated on a continuous basis, 'reassembled and targeted', or whose data are offered in the market of behavioural control are deprived of the capacity to act autonomously. This is because their actions are steered by service providers. This results in the lack of autonomous actions which was the common element of problems described in the previous section: manipulation, coercion and discrimination. Autonomy is also infringed because of the mechanism called 'filter bubble',[357] or 'autonomy trap',[358] the result of putting individuals into an environment based on their data from the past reflecting pre-existing beliefs and inclinations. Such an environment is created, for example, by algorithms regulating what is seen on social media or in search results. This deprives people of surprise and serendipity which help them to learn and develop.[359] This also impacts on their ability to create new ideas, because this ability depends on the freedom of thought and beliefs, engaging freely in intellectual exploration, and the confidentiality of communications with others.[360] All of those elements are compromised in the online environment which deprives individuals of some choices.

Furthermore, surveillance deters individuals from doing things which they would otherwise do. This works through influencing the life of individuals who are aware of increased risk of 'undesirable' behaviour and try to minimise it by altering their behaviour, which is often called 'a chilling effect'.[361] Very similar, albeit only indicative, insight about surveillance may be obtained from the literature, for example from *1984* by George Orwell, *Brave New World* by Aldous Huxley, or *Cancer Ward* by Alexander Solzhenitsyn (quoted at the outset of this thesis). But such behavioural control may also work through more invasive methods of manipulation, for example, by not providing necessary information to make an informed decision, or by hiding commercial aspects of some activities. The harm arises from the invasion of individuals' activities and not allowing them to autonomously determine their life choices.[362]

---

[357] Pariser 2011.

[358] Zarsky 2002.

[359] Thaler and Sunstein 2009, p.99.

[360] Richards 2015, p.108.

[361] Solove 2008, p.178.

[362] Solove 2006, p.73.

Second, the surveillance models show dignitary harm caused by surveillance which can be perceived as disrespectful or demeaning. This starts with the language used for online activities. The language of online businesses is distant, arrogant, and treats market and interaction with customers as a battlefield.[363] The marketing jargon is full of expressions like 'eyeballs'[364] or seats (for people), customer branding (for making people remember products), targeting (for addressing some group), capturing traffic (for redirecting people to other websites), capturing value or generating sales (for selling products), getting hits (for customer 'visits'), conversion rate (for the number of people who took desired action), or demographics (for information about customers). This is language in which the human is not treated as a subject, an end in itself, but rather as an object of actions aimed to 'monetise the value of data'. Dignity may also be infringed as a result of opacity of algorithms and the approach of the companies to not inform users about the logic behind those algorithms.[365] When nobody is able to explain the reasons for a decision in a meaningful way (besides 'the computer said so' or 'it is in the system'),[366] people feel manipulated by unexplained power, which bears resemblance to another masterpiece of literature – *The Trial* by Franz Kafka.

Also, possessing vast amounts of personal data is like holding power over data subjects. These data are not gathered in the interests of people, but used as a means for commercial interest. Commercialising personal data which may reveal personal characteristics of individuals may be considered degrading or demeaning.[367] For example, controlling what individuals read or search for on the web means essentially controlling what they are thinking. The websites, applications and e-book readers, like Amazon's Kindle, gather detailed information about their interests. Sometimes they know what page users are on, how much time they spent on each page, and what they highlighted. It seems that the books or newspapers are reading the readers.[368] Such information was traditionally kept private.

---

[363] Levine and others 2000, p.78 ff.

[364] Eg House of Lords ("Oral evidence from David Evans and Ariel Ezrachi") 2015, p.3.

[365] 'Are you being optimised or monetised?', see Angwin and others 28 September 2016. To some extent this logic may not be known, for example, in the case of 'machine learning'.

[366] See the examples of the algorithms governing teachers' evaluation and supporting the justice system in assessment of probability of re-offending in O'Neil 2015; also, Korff and Brown 2013, p.22.

[367] Sandel 2012, pp.186–189.

[368] Richards 2015, p.129.

Last, but not least, the most serious and obvious infringement of dignity is when someone's personal data revealing intimate information is published to the world.[369] In such cases the distress for individuals is often very severe, as disclosure distorts others' judgement about them, makes them "prisoners of their recorded past" and prevents them from social interactions, and normal development.[370] However, this effect is subjective, and some individuals may decide that they want to disclose their intimate details to the world (celebrities, for instance). The regulation preventing them from doing so would be unduly paternalistic. In other words, 'the right to make bad privacy choices' should be preserved.

3. *Interference with social values*

All the problems described above in the two previous sections are related to individual values. But, as indicated in Chapter II, privacy can also be valued as social or public good. The privacy problems related to interference with these values are often overlooked. This is because privacy is seen only as an inherent feature of individuals and, therefore, according to a public–private dichotomy, contraposed to public goods.[371] Such a view is oversimplified because privacy is necessary for interactions between individuals, and such individuals constitute society. Therefore, privacy problems inevitably have a social dimension which cannot be underestimated.

Firstly, some impediments to autonomy like the 'chilling effect' also affect society as a whole, as people do not possess the free space necessary to develop not only themselves but also socially desirable ideas.[372] This is the case with freedom of thought which also underpins many

[369] Eg Solove 20 March 2016; Hern 14 March 2017; "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner - Office of the Australian Information Commissioner (OAIC)" n.d.

[370] Eg Solove 2008, pp.143–145.

[371] In such views, the use of data is necessary for the public good and what holds it back is private interest, eg Chapter 6, Australian Government, Productivity Commission (No. 82) 2017.

[372] Solove 2007, p.19.

other freedoms, for instance, freedom of speech.[373] Freedom of speech is affected on societal level by the chilling effect when people are aware of surveillance. It destroys their comfort which leads to self-censorship. This is why surveillance was used in history by totalitarian regimes to control people and societies. For example, during martial law in Poland in 1982, phone users could hear at the beginning of each phone conversation an automatic announcement that 'the call is being controlled'.[374]

Secondly, as pointed out by Solzhenitsyn:[375]

> Something negative or suspicious can always be noted down against any man alive. Everyone is guilty of something or has something to conceal. All one has to do is to look hard enough to find out what it is.

So, the corporate surveillance creates a perfect base for what Russians call 'kompromat', a word coming from 'compromising material'. Collecting data about everybody means that everybody can be manipulated or coerced by those who have data. This clearly allows those holding the data to stifle the self-development of society giving them more control over others. Furthermore, it may be claimed that large collections of behavioural data are a public hazard,[376] especially if they are improperly protected. This is because they can be exploited by anyone who finds a way to copy them and use them for the detriment of individuals and society.

Thirdly, there are clear signs that personal data collected by online services are used for social manipulation. For instance, Facebook was conducting research which consisted of manipulation information for users for scientific purposes.[377] They were manipulating people's 'news feeds' measuring how this affected their mood. Also, that social network can influence voting in democratic countries, not only by mobilising certain people to

---

[373] Contrary to the popular belief that privacy is always opposing the freedom of speech and has to be balanced with it.

[374] Also, the use of surveillance in East Germany in the movie *The Life of Others*.

[375] Solzhenitsyn 2003, p.209.

[376] Cegłowski 2016.

[377] Kramer, Guillory and Hancock 2014.

participate,[378] but by clearly addressing them with political messages,[379] which may be adjusted to their psychographic profiles,[380] and sometimes completely false ('fake news'). This trend may have even longer-term consequences as, according to Zuboff, 'surveillance capitalism' is inherently anti-democratic, because it structures the firm as formally indifferent to and distant from democratic populations.[381] It has to be added that global corporations become a new sort of international power to which some countries are already sending ambassadors,[382] and their leaders may have political ambitions.[383] It may be slightly too early to say that this is the installation of a new kind of sovereign power,[384] but the power of those companies is linked with an unprecedented lack of accountability. Furthermore, the Internet is a network which substitutes previous networks of exercising power (broadcast media, education, knowledge, communications, technology),[385] and gatekeeper companies are effectively mediating many relationships between people, and between those who govern and those who are governed. So, the implications for society and democracy of shifting the 'centre of gravity' to the Internet without informational self-determination may be serious.

D Conclusions

This chapter has described the *modus operandi* of online service providers and privacy problems which result from their actions. They compete to design an online market in a way which puts them in a position to control personal data and data flows. The use of those data to deliver to individuals the requested service by subjects who are known to them does not infringe informational autonomy. However, it starts to become problematic when individuals are tracked, profiled, and their data exchanged with third parties (eg data brokers).

---

[378] Bond and others 2012.

[379] See 'The Computational Propaganda Project' at Oxford Internet Institute n.d.

[380] Concordia 2016; the research shows that this actually may work, Kosinski, Stillwell and Graepel 2013; Youyou, Kosinski and Stillwell 2015; however, whether such methods have already been used remain to some extent unclear, Doward and Gibbs 4 March 2017.

[381] Zuboff 2015, p.86.

[382] Baugh 2017.

[383] Lee 19 November 2016.

[384] Zuboff 2015, p.86.

[385] Traditionally controlled by governments, Foucault 2000, p.123.

Unfortunately, the exchange of personal data with third parties is the basis for the most successful business models in the Internet economy (ie the non-trading platform) and the result is a 'stalker economy'.[386] In such an economy, the value of personal data is derived from the ability to influence (or manipulate) data subjects.

This causes a deep inequality in the relationships between online service providers and data subjects, because the field of interaction is not a public space, but a privately owned architecture created and fully controlled by service providers. It is designed to pursue their commercial interests by leaving individuals with limited choices when they are led through the steps of their pre-defined 'customer journey'. The game is about putting individuals in a position in which they have to choose between participation in a digital society and keeping their personal data away from extensive corporate surveillance. This is not a free choice (and freely given consent), because asymmetry of power and knowledge does not allow customers to 'see' what is happening on the other side of the network. But, they are individualised, fully 'transparent' to service providers and, therefore, exposed to their actions.

The detriments flowing from such activities are compound and serious. First, there is a structural risk of tangible loss bound up with data activities which increases as data move along the steps of their processing cycle. This may result in discrimination, manipulation, coercion, or 'identity fraud'. Second, there is harm to the personal values of autonomy and dignity. As a result of corporate surveillance, individuals' behaviour is modified, 'chilled' by auto-correction, and they are deprived of free choice. This is not only disrespectful and demeaning, but impacts on their ability to create new ideas, learn and develop. And, third, there are significant detriments to social values. This is because privacy is the internal element constituting society, and databases of personal data may be used to influence individuals and, by those means, the whole of society. They are simply a public hazard.

So, all the above not only gives a rationale for a corrective action, it shows exactly which activities are problematic. It also suggests that such corrective action should work against the mechanisms shifting power towards online services. That is to say, there need to be

[386] Levine 11 June 2014.

countermeasures focusing on architectural and informational imbalances. The following chapters show how to construct and adopt such countermeasures.

PART II

THE SOLUTION:

PRIVACY MANAGEMENT

IV How to Regulate Online Services

The previous chapter, and indeed Part I as a whole, has shown that online services have systemic problems resulting from pervasive personal data collection and processing. Those problems clearly require some regulation, which should lead, consistently with the thesis title, to construction of an effective privacy management system. Regulation is understood in this thesis broadly, as all intentional interventions (ie control, order, or influence) which aim to alter the behaviour of others according to the defined standards or purposes in a sustained and focused way with the intention of producing some broadly defined objective.[387] This is to encompass as many actors that influence online privacy behaviours as possible and as many possible methods of influence.

Such regulation should be responsive to the regulatory environment and understand the context and motivations of those who are to be regulated.[388] There are various possible models of such responsiveness.[389] Braithwaite suggests that there is no tightly prescriptive theory of such regulation and that it should rather be grounded on the practical problems present in a given industry.[390] In keeping with that view, this thesis does not aim to set out any novel framework nor to resolve any debate about regulatory models or modes of regulation.[391] It only aims to find a practical response to the deficiencies outlined in Part I. Those deficiencies come from the economic incentives of market players and are strongly related to the ICT architecture. This is the peculiarity of the regulation of technology to which writers often respond by referring to regulating forces (developed by Lessig)[392] – law, market, norms, and 'code'.[393] This thesis will refer to some ideas from this model, but it will not be adopted in its

[387] Black 2002, p.26; similarly, Baldwin, Cave and Lodge 2012, p.3; Frankel and Yeabsley 2011, p.2; cf Freiberg 2010, p.4.

[388] Braithwaite 2017, p.118; Drahos and Krygier 2017, p.5.

[389] See Braithwaite 2017, pp.118–128.

[390] Braithwaite 2017, p.130.

[391] Review of such discussions, Drahos 2017; Braithwaite 2008.

[392] Lessig 2000.

[393] Eg Chang and Grabosky 2017, p.535; Brownsword and Yeung 2008, p.1; Rowland, Kohl and Charlesworth 2017, p.11.

entirety. Instead, it will be used to devise a 'smart', complementary set of regulatory tools[394] to respond to the problems described in Part I of the thesis.

This chapter draws a detailed plan of this kind of regulation of online services. Part A defines objectives – what effective regulation should achieve – and explains the main problems which need to be overcome in order to regulate privacy effectively. Then, following the discussion in Chapter II, it defines the Privacy Management Model (PMM) and its main functions: organising, planning, controlling.[395] It explains how this model should regulate online services to enable effective privacy management, and shows the relevant test for checking that its aims have been achieved.

Part B answers the question why PMM should underpin the regulatory tools designed to protect individual privacy. The arguments raised cover ways to remedy problems (relating to both privacy values and to the correction of market failure), and also explain that PMM forms an effective mechanism for facilitating the interaction between data subjects and online service providers and for creating a safe environment where transaction costs are reduced. It offers a win-win solution for data subjects and service providers, because individuals get better and more convenient control over their privacy processes, while trustworthy online service providers get less risky and more flexible access to data.

Part C focuses on the regulatory tools which can implement PMM and, in so doing, introduces the following chapters of this thesis. It recognises that PMM should be implemented using a regulatory mix of market regulations, technology (also the 'code' or architecture), and law. It describes how those tools should be applied to introduce PMM. Furthermore, it shows which regulatory regime could do this most successfully.

A Regulating Privacy with Privacy Management Model

This thesis focuses on regulation of the specific relationships between data subjects and online service providers. These relationships are based on the private interests of two parties, who

[394] Gunningham and Sinclair 2017, pp.134–135.

[395] Betkier ("Individual Privacy Management") 2016, p.323 ff.

come to the transaction to achieve reciprocal benefits. Even though what is actually exchanged, personal data, cannot be limited to commercial value, still, the exchange has a commercial character and is usually based on a contract between the parties.[396] So, what are the goals that regulation should achieve?

1. *What privacy regulation should achieve*

The goal is set specifically on effectiveness of the regulation of the relationships in question. Usually the assessment of regulation is done on the basis of a mix between substantive criteria (such as conformance to natural justice principles, moral values, human rights, or rule of law), and criteria related to results.[397] The latter usually include effectiveness.[398] Effectiveness, as explained by Freiberg, addresses the issue of whether desired regulatory objectives have been achieved.[399] This approach is taken here for several important reasons. Firstly, the failure of consent is a problem of lack of effectiveness of this method of individual authorisation in exercising autonomy. As shown in Chapter II, rather than being effective, consent is a mere procedural tool which is viewed as a pure formality by both parties. Secondly, an effective mechanism for exercising individual autonomy is necessary because of the importance of values protected by data privacy: dignity, autonomy, and public goods such as democracy. So, one goal of this thesis (values-related) is to devise a solution which effectively protects those values. Thirdly, as there is no way back from automation of information processing, it must be possible to implement data privacy regulation in the digital economy. Therefore, it must also be effective for service providers, which forms the second goal of this thesis (economics-related).

Effectiveness is a difficult criterion to assess in the context of regulation since it refers to the clear statement of objectives and their consistent understanding in the whole regulatory system.[400] As both types of effectiveness (ie values-related and economics-related) are broadly

[396] Eg Kim 2013, p.59. However, a service can be based on statute, for example, for services provided by state agencies. Also, the fact that online tracking by the third parties is validly based on contract may be questioned.

[397] 'Non-instrumental values' in Freiberg 2010, pp.263–268; Koops 2008, p.168.

[398] Freiberg 2010, pp.260–263; Koops 2008, p.168; Bennett and Raab 2006, p.244.

[399] Freiberg 2010, p.260.

[400] Bennett and Raab 2006, pp.245–246.

defined, there is a need to make some assumptions to operationalise them. Firstly, values-related effectiveness will be evaluated by the actual ability of data subjects to manage their own data. This can be measured by the ability to plan, organise and control data activities by data subjects. Relevant test (objectives) will be presented after the presentation of the Privacy Management Model in section 3. Secondly, the evaluation of economics-related effectiveness needs to refer to the effective operations of the 'data markets' enabled by using personal data. In other words, personal data must continue to "oil the wheels" of digital economy, "not to put spanner in the works".[401] The way in which the regulation presented here achieves economics-related effectiveness will be thoroughly discussed,[402] but it can only be verified after its implementation.

These two elements of the effectiveness criterion, effective management of personal data by data subjects and effective market operations, seem on the surface to be hard to reconcile, but a win-win solution is achievable. At first glance, it seems that what is provided to data subjects to manage personal data is at the expense of service providers. For example, they need to create the functionality to manage individual privacy processes in their systems.[403] But, although exercising the personal autonomy of data subjects obviously affects business models of service providers by limiting the way they can process personal data, it may not only be a limitation, burden, or restriction on them. It could also be a measure which acts to manage the risks of both parties of the relationship, enables and facilitates their interaction, and creates safe environment reducing transaction costs.[404] Perhaps, data privacy laws may function similarly to the policies of 'sustainable development' in environmental protection, reducing the potential for conflict between two sets of interests.[405] For example, autonomy of both parties is exercised in contract law, which by the means of rational planning serves the market mechanism to achieve efficient allocation of the resources.[406] So, re-introduction of balance to the relationship in question may be a way forward.

---

[401] Goff 1984, p.391.

[402] In Part B and the next chapter.

[403] Similar to ISO/IEC 29101:2013.

[404] Freiberg 2010, p.2; Baldwin, Cave and Lodge 2012, p.3.

[405] Bygrave 2001, p.282.

[406] Eg Brownsword 2006, p.49 ff.; Trebilcock 1993, p.7.

So, the goal of the thesis is to achieve effective privacy management. This may be achieved when privacy regulation influences the way data subjects exercise their informational autonomy to overcome consent failure and create a safe environment where data transactions are performed effectively. Knowing what the goal is, it is time to summarise the typical problems of data privacy regulations because they need to be overcome.

2. *Problems of data privacy regulation*

There are some particular problems related to data privacy regulations which make them challenging. They are presented below with a discussion which introduces the characteristics of the Privacy Management Model presented in the next section.

The first of the challenges in devising regulations of data privacy comes from its subjectivity which makes it difficult to define rules about data. As discussed in Chapter II, the value and sensitivity of personal data are different for different people in different contexts. They change in time, depend on the personal characteristics of data subject, social roles, and on other factors such as availability of other data or, importantly, the goal which data subjects want to achieve by using their data. For example, as mentioned in Chapter II, celebrities share a lot about themselves as they receive more attention which converts into more opportunities to monetise their popularity. Probably on the other side of the 'privacy spectrum' would be a public prosecutor or a criminal judge who may like to separate their professional life and people they have to deal with professionally from their private and family life. Also, the sense of dignitary harm is to some extent subjective. For example, some people may be more vulnerable to the harm resulting from public disclosure of their intimate affairs than others. So, this all suggests that the valuation of privacy bargains should be left for data subjects, as they are in a position to make the best decision about the use of their data. However, this is difficult because, as discussed in Chapter III, individuals lack expertise in assessing their own privacy choices and are put in a disadvantageous position.

An alternative idea is to use an objective standard of privacy. This is the current approach of service providers who dictate the T&Cs and for some choices use common default privacy settings on a global level which, as noted above, promote data 'sharing'. A mixed objective-subjective model is the standard used by courts as the 'reasonable expectation of privacy'

criterion (or test) to assess privacy expectations of individuals.[407] Such a societal standard may be understood as a set of privacy choices[408] that an individual might exercise which would be uncontroversial for most of society members.[409] But, this standard brings many difficulties related to a fully subjective approach. This is because it depends on the community the person lives in, the professional group they belong to, and the society they live in. Some authors segment society into different privacy attitudes, such as privacy fundamentalists, pragmatists, and unconcerned.[410] Some communities may also be particularly vulnerable or exposed, which may be a case of different minorities, for example ethnic or sexual.[411] Finally, the sense of privacy differs globally between continents (eg in Europe and in America),[412] and also between specific countries.[413]

So, as online services are global, there needs to be some way to adjust the global privacy 'standard' of service providers to subjective choices of people. It seems that the decisions as to data collection and use should be left for individuals to make, but the regulatory system, ideally, should have built in some way of supporting them with necessary skills, expertise, and a neutral set of default privacy settings adjusted to their society or even community. Such support should be provided by third parties, because the incentives of service providers are to increase collection.

Second, and probably the biggest, problem for privacy regulations (in devising rules and enforcing them) posed by the online environment is the problem of factual control over information.[414] It is said that the main characteristics of information are that it is non-rivalrous and non-excludable.[415] This means that 'consumption' of information by one person does not prevent 'consumption' by others and that it is very hard to prevent people from copying and

---

[407] Moreham, Warby, Tugendhat and Christie 2016, pp.49–51; Gomez-Arostegui 2005.

[408] Note that the legal test of reasonable expectation of privacy is more than just this, Moreham and others 2016, pp.50–51.

[409] Eg *Hosking v Runting* [2004] NZCA 34, para.250 as per J Tipping.

[410] Westin 2003, p.445; also, discussion in Urban and Hoofnagle 2014.

[411] Eg Korolova 2011.

[412] Whitman 2004, p.1161; Cohen 2000, p.1423.

[413] More broadly in Koops and others 2016.

[414] Solove 2008, p.28; boyd 2012, p.349; DeCew 1997, p.53.

[415] Acquisti, Taylor and Wagman 2016, p.446; also, Spiekermann et al. 2015, p.162.

distributing it. And, as often claimed in discussions around intellectual property, "information wants to be free",[416] which corresponds to the ease of copying and transferring data. So, it is hard to control the onward transfer ('downstream use') of personal data to third parties and there might be no sign that they have been copied.[417] Furthermore, those third parties may create databases of personal data invisible to data subjects, and, therefore, not possible to be managed by them. However, the use to which personal data have been put has an impact on their economic value. For example, there is no point in presenting advertisements to the customer who already has bought a given good. So, online companies do not willingly share personal data, because they would lose their value. To prevent this, as recognised in Chapter III, they compete by *excluding* their databases for their own use.[418] They do not run open systems like the Internet, but closed systems. Despite the popular account about non-excludability of the information, those personal data which have value for service providers are de facto excluded from public access, secured, and stored in their centralised, 'hub and spoke' systems (compared to bank accounts in the previous chapter). Data can be subject to regulation in the place where they are located. Such regulation, as discussed in Chapter II, should be based on managing them.

So, the focus of data privacy regulation is on managing data collection and use, which should be done in the place where those data are stored. Managing data covers inter alia controlling data and protecting them from being transferred. Usual ways of protecting data rely on limiting their availability (by restricting access, decreasing their visibility,[419] minimising collection, or deleting), limiting their usability (eg by removing their important features, such as class designations, or anonymisation of data), limiting their use (eg by assigning and enforcing policy of use), or keeping the track of data operations (eg by logging records of such operations). Those methods are usually exercised *directly* by the data controller (ie service provider), and have a physical, technological nature. But, there are also indirect methods of control, which may be exercised by the data subject as visualised in Figure 10 below by the means of actual data controllers.

---

[416] Attributed to Stewart Brand, Wagner 2003, p.999.

[417] 'Cross-platform transfers' in Jones 2016, p.187.

[418] Stucke and Grunes 2016, p.45; Graef 2016, p.267.

[419] Eg removing them from the search index, Case C-131/12 *Google Spain* [2014] CJEU.

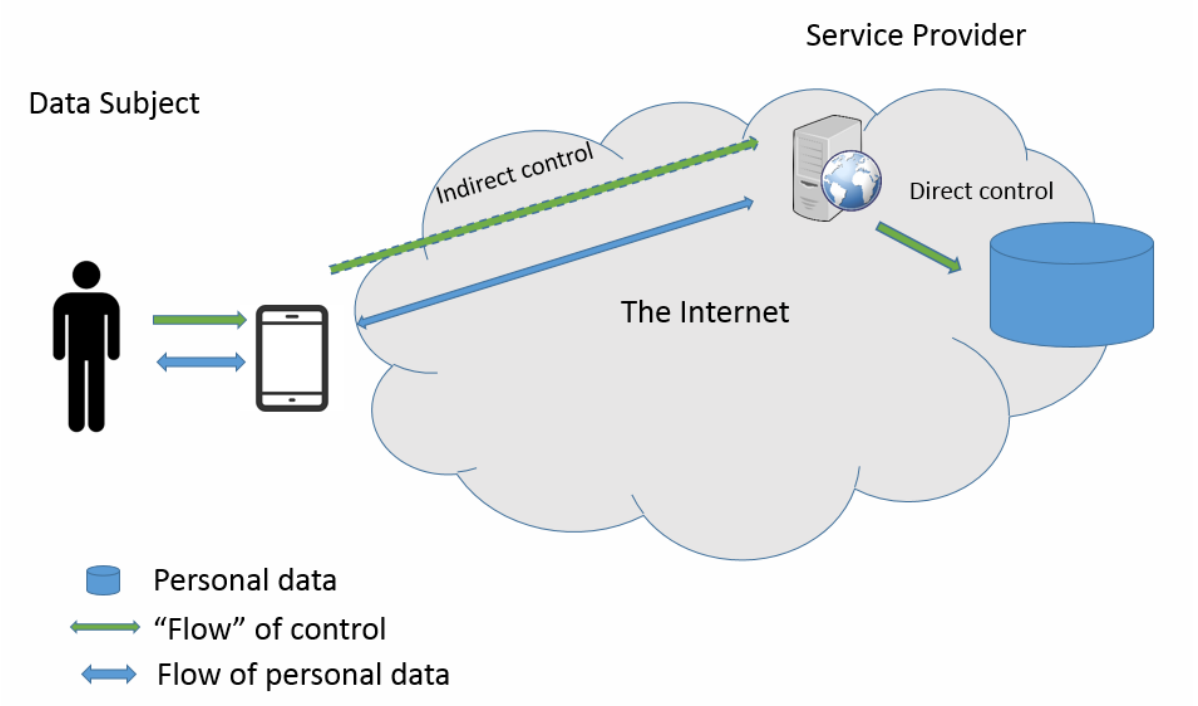


Figure 10 Direct and indirect control over data

For example, the so-called 'purpose limitation principle' which may be traced in many data privacy laws around the world[420] is in fact an *indirect* method of control limiting use of data by the data controller by the means of legal rules. This is because it relies on obtaining data subjects' consent[421] for data use for a particular purpose disclosed at the moment of giving this consent. When consent is given, use for that particular purpose is permitted, while use for other purposes is not permitted and may require additional consent. Furthermore, such a legal measure should have reflection in the data controller's physical limitations of data use. Another example of an indirect method of control are privacy settings used by data subjects via the interface ('privacy dashboard') on the service provider's website which, for example, restrict some data use. This indirect method of control uses technology (architecture). So, control over personal data by the means of regulatory methods may be direct or indirect and may be exercised by both parties.

The third significant challenge in formulating data privacy regulations comes from the fact that they usually pertain to different types of data controllers with different interests in using

[420] DPD, Article 6(b); principle 5 in PIPEDA. More in Chapter VII.

[421] Sometimes knowledge is enough, OECD Guidelines 2013, s 7.

personal data.[422] That is to say, omnibus privacy laws usually refer to private interests and, jointly, public interest in personal data. Limiting the scope of the thesis to private interests, as explained in Chapter II, enables it to concentrate on the exact nature of problems with online services. In this way it avoids involvement in the exercise of balancing privacy with other values, such as freedom of expression or access to information.[423] But, the proposed solutions need to be compatible with the 'public half' of privacy regulation. So, individual control over collected data should be limited where they are collected or used according to particular public interest. For example, data about telephone connections may need to be retained for the purpose of crime detection and cannot be deleted, even by data subjects. However, as will be shown below, it is possible to recognise such limitations without undermining privacy management of other personal data.

In conclusion then, data privacy is hard to define by legal rules, which suggests that the valuation of privacy bargains should be to a large extent left for data subjects, but the regulatory system should find some method to support them with necessary skills and expertise by third parties. The problem of factual control over information may be solved because personal data are excluded in the ICT systems of service providers, so they can be indirectly managed by data subjects there (with some limitations related to public interest). So, what should this effective, indirect management look like?

3. *Privacy Management Model*

The tool for management of personal data, Privacy Management Model (PMM),[424] is a set of functions necessary to manage the privacy process. PMM forms a theoretical model to implement autonomous choice in respect of a data process. It builds up the idea that, as

---

[422] However, in some countries, such as Australia and Canada, those regulations were in the past, or even currently are, separated.

[423] Such balancing may be complex, eg "The Advisory Council to Google on the Right to be Forgotten" 2015, p.4 ff..

[424] This is the extension and revision of the model described in Betkier ("Individual Privacy Management") 2016, p.323 ff. Changes include eg: evaluation criteria, the adaptation of planning to the external and dynamic use of privacy policies, better links with theoretical backgrounds, new categories of data and data uses.

explained in Chapter II, managing the privacy process provides the highest level of autonomous choice. As outlined there, privacy management requires:

- Controlling, with the ability to monitor the process and reflect on its state;
- Planning, as the ability to 'look forward' and set goals (individual policy);
- Organising, as structuring the key parameters of the process and access to them to perform other functions.

Managing privacy should be a process as only a process can effectively control another process. This is because controls have to be adjusted to the changes of external circumstances and changes of plans. For example, the process of driving a car is managed by the process which controls the car by the means of continuous manipulation of several crucial parameters of the car's operation, such as speed, gear, or wheel turn.[425] Some of those parameters are monitored and results are presented to the human operator. The car controls are constructed (organised) in a way which enables effective control (dashboard with indicators, steering wheel, etc). Planning is performed by the driver who uses the car to reach some destination, exercising one's particular goal.[426] A similar set of functions is needed to manage a privacy process. The functions of privacy management are more than interrelated; they are interlocking, so they rely on each other for the effective management to operate. They are described in Figure 11 below.[427]

[425] This can be to a different extent automated, but then those tasks are performed by the machine steered by a human, eg Christensen and others 2015.

[426] Some elements of planning may also be automated, for example, by using GPS, or by relying on some element of car automation, ibid., p.11.

[427] Cf Betkier ("Individual Privacy Management") 2016, p.324.

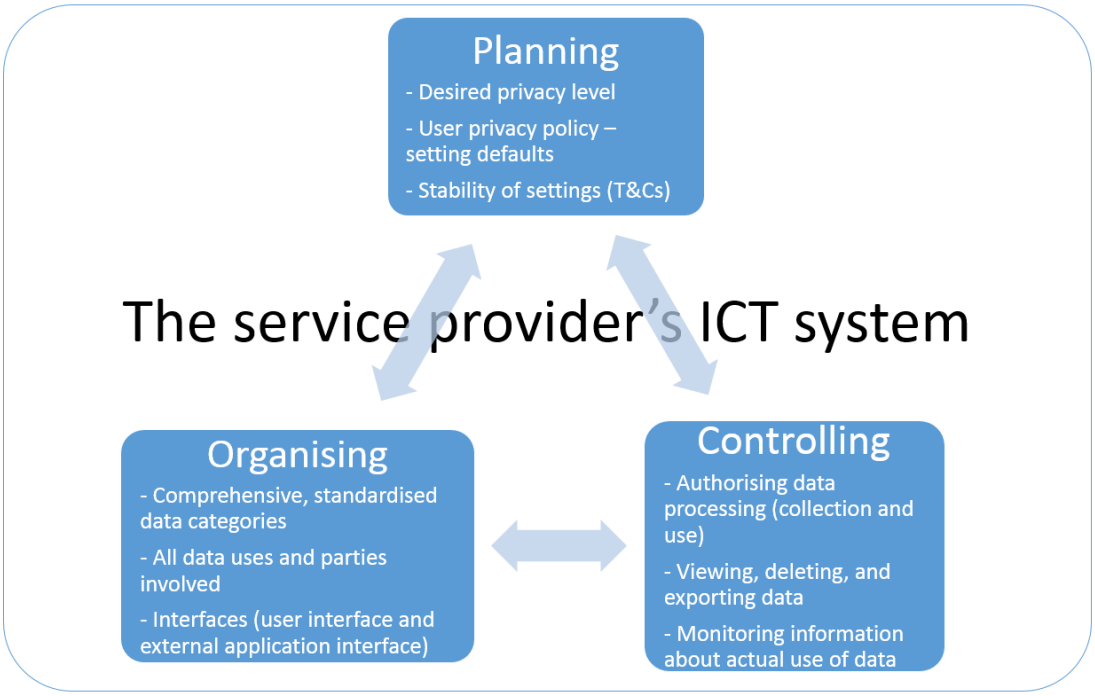


Figure 11 Privacy Management Model and its functions

The idea of PMM is based on indirect control over data presented above. So, data subjects manage their data privacy processes through the 'agency' of service providers who keep personal data. Such control is exercised in the service providers' ICT systems by the means of technical and legal tools, which will be presented in the following chapters. What are those functions?

The main idea of planning[428] is that data subjects can set their own plans about the way their data are to be collected and used, to express their subjective expectations about their privacy. Their expectations should have precedence over objective, societal expectations of privacy used as default privacy settings. Such a set of preferences (ie societal, default settings with changes resulting from individual privacy expectations) form the privacy policy of the individual which should override any 'system settings' provided by service providers. To achieve privacy goals embedded in their privacy policy, data subjects need stability of those settings which is nowadays dependent on stability of the provisions of T&Cs (containing basic definitions and declarations about data use). In PMM, privacy settings should be set and monitored from *outside* the ICT systems of service providers. In this way, individuals regain authority over their own data, assuming that those data and ICT systems holding them are properly organised.

[428] Betkier ("Individual Privacy Management") 2016, pp.324–325.

The organising function in PMM[429] is based on adopting comprehensive and standardised categorisation of data and data uses. Such categorisation makes it possible to align the expectations of both parties as to the exchanged data and their purposes. This is because they will refer to the same standardised definitions. This is a crucial part, as currently every service provider offers its own, usually very complex, way of defining categories of data and data uses. Organising includes also providing data subjects with interfaces enabling them to access their privacy settings and to manipulate those settings (to exercise controlling and planning). There should be two such interfaces, one oriented on direct control by data subject (User Interface, UI), and the second one (Application Programming Interface, API) oriented on indirect, automated control by the means of some external, automated software used by data subjects or a third party[430] acting on their behalf. This is the way the privacy policy of the individual gets into the ICT systems of service providers.

Controlling[431] is a broader set of activities currently entrusted to consent. Data subjects should be able through controlling function to authorise processing of different types of their personal data (ie their collection and use). The difference between controlling function of PMM and consent is that consent authorises data uses upfront for the purposes predefined by the service providers (and often later unilaterally changed by them[432]), while controlling function authorises collection of particular standardised (organised) types of data and their particular uses giving data subjects a constant ability to change those decisions in the course of the relationship. Also, controlling should be possible in relation to already collected data. Data subjects should not only be able to see them, but also delete (without leaving additional copies) or export them, for example to use them with another service provider (data portability) for their own goals. Furthermore, controlling should enable data subjects to monitor those data and their uses and to reflect on that use to reshape their own privacy goals (in planning).[433] Monitoring and enforcing privacy by individuals in the ICT systems of service providers are

[429] Betkier ("Individual Privacy Management") 2016, pp.325–327.

[430] There should be a suitable 'business model' (arrangement) for such third parties to operate. See Chapter V.

[431] Betkier ("Individual Privacy Management") 2016, pp.327–329.

[432] Despite 'purpose limitation' (or 'use limitation') service providers are the masters of current T&Cs. Chapter VII gives detailed examples how changes of T&Cs influence users.

[433] This bears some resemblance to the vision of the medical system described in Zittrain 2000, pp.1243–1244.

probably the hardest to achieve, although, as will be argued in the Chapter VI, new technologies give tools and ideas how that could be exercised. Also, there are other limitations to controlling. As recognised in section 2 above, some actions would be not possible for data and data uses needed for public goals. For example, deleting data reserved for law enforcement should not be possible in the time frame in which relevant legislation orders keeping them available. There is, however, no reason to hide those data from data subjects[434] or to allow other uses of those data against data subjects' informational autonomy.

Ideally, privacy management should enable data subjects to dynamically manage data according to the cycle of activities presented in Figure 12 below.[435]

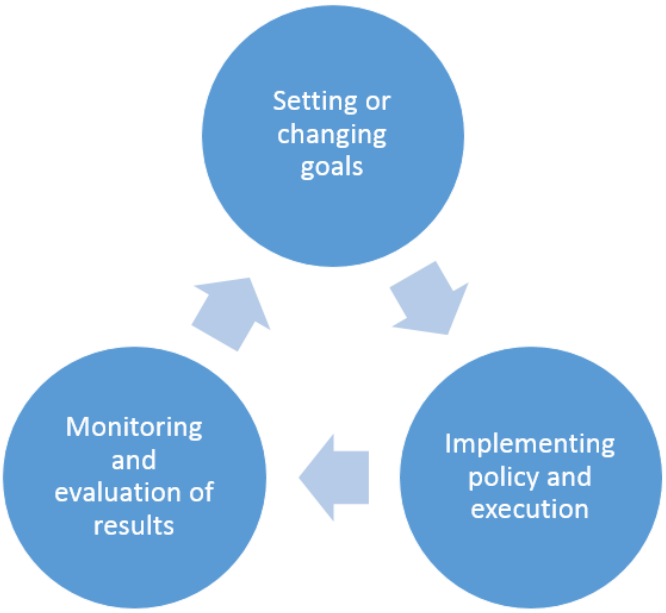


Figure 12 Privacy management cycle

Those activities are similar to business management activities and enable data subjects to reflect on the achievement of their goals and to adapt their decisions to external circumstances. The idea behind this is that these functions should enable them to effectively manage their data, and not just have a feeling of control.[436] Consequently, in this way data subjects could be able to some extent ascertain (and decide) who knows what about them (achieve informational self-determination).

---

[434] There might be some cases in which data should not be accessible by data subjects (eg state secrets, protection of vulnerable data subjects), but these should be treated as rare exceptions.

[435] Betkier ("Individual Privacy Management") 2016, p.328.

[436] Cf Tene and Polonetsky 2013, p.261.

PMM would constitute a separate mechanism from consent applicable to providers of Internet services who potentially breach informational autonomy (as described in Chapter III). In this view, those businesses would implement and maintain necessary data organisation structure and interfaces enabling individuals to manage their data from outside of service providers' environments. Management could be exercised by data subjects supported by third parties. To enter into a relationship with such online service provider, when concluding online contract data subject should enable (authorise) such service provider to import user data policy settings (individual privacy policy) from a system which is directly or indirectly controlled by the user.[437] In this way, the default privacy settings of the user take precedence over default settings of the online service. Furthermore, the service provider should also enable (authorise) that system to perform further, ongoing management of privacy for particular data subject. Nevertheless, potential collection and use of additional personal data could be freely negotiated by the parties, but would require additional action from the users to change some part of their privacy policy and, as such, could be exercised by the means of the third party.[438]

The key aims of the model outlined above can be reflected in eight questions presented in Figure 13 below.

[437] See the model of interaction with a third party in the next chapter.

[438] Only if the data subject wishes to do so.

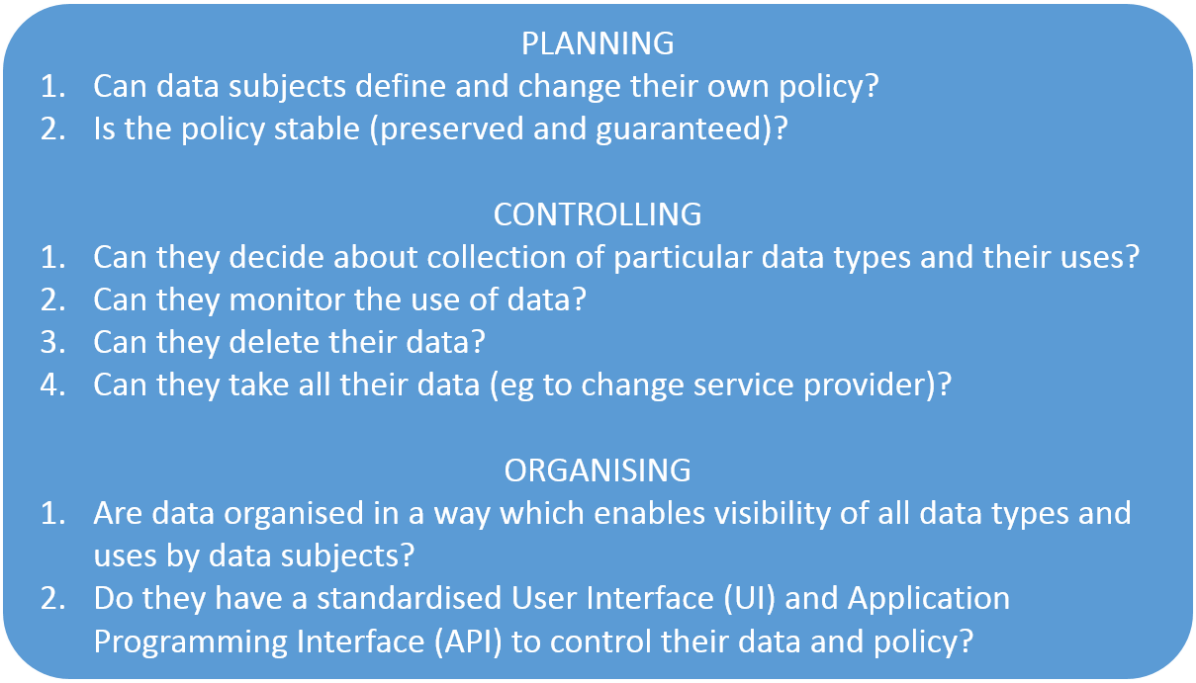


Figure 13 Evaluation criteria for data subjects' autonomy in Privacy Management Model

These questions constitute evaluation criteria to verify if data subjects can effectively exercise their informational autonomy with PMM. This is because these questions check that all relevant functionalities of PMM are delivered. They will be used throughout this thesis to develop and verify the proposed mechanisms of regulation implementing PMM.

Implementing PMM could allow to deemphasise the overcomplicated[439] consent procedure. As a result, consent could be very simple as it would not be the only way in which data subjects could exercise their autonomy. The possible benefits of introducing PMM-based tool for privacy management are described in the next Part. To be implemented, PMM requires a mix of functionalities delivered by particular business model and by technology tools. This mix is introduced in Part C and described in detail in the following chapters.

B Why Regulate Privacy with Privacy Management Model?

There are three main groups of benefits of implementing PMM: achieving values-related goals, correcting market failures, and achieving positive goals for a digital economy. This corresponds to the division in privacy values and privacy problems to non-tangible and

[439] By the provision of additional unnecessary information, and multiple, separate consent statements.

tangible ones, but also splits economic arguments between argumentation showing advantages for individuals and for businesses. Those benefits are assessed according to the effectiveness criteria outlined above, and also help show how a regulatory discussion around privacy is likely to develop. They form a 'toolkit' of arguments which could be used to support the idea of PMM.

1. *Achieving values-related goals*

Values-related goals (protection of dignity, autonomy and social values) may be achieved by strengthening the position of data subjects in relation to service providers. Firstly, and most importantly, implementing additional means for privacy management may be justified by the need to ensure respect to individual values, such as self-determination or autonomy,[440] so implementing effective privacy management. In this respect, PMM explicitly aims to strengthen the autonomy of the individuals by giving them tools to manage personal data. Such an explanation is likely to be powerful in countries where liberal values are very important. This might seem paradoxical, because belief in individual liberty goes often together with belief that government should not regulate the market as there is no reason for it to know better what is in the interest of individuals.[441] But, even in the minimalist view of a night-watchman state, privacy regulation may be justified as one of the important guarantees of individual freedom. As such, it may be argued, it is required to restore the balance of power and make sure that data transactions are at arm's length. As the privacy problems are systemic, they require a systemic solution such as PMM.

As discussed in Chapter II, this individual freedom may be presented as a 'freedom to' or, 'freedom from'. The 'freedom from' version of privacy protection is recognised as a human right in Article 12 of the Universal Declaration of Human Rights (1948) and in Article 17 of the International Covenant on Civil and Political Rights (1966). It relies on protecting individuals from arbitrary interference with their privacy. Examples of constitutional-level privacy rights presented as 'freedom to' are the German right to informational self-

[440] Sunstein 1990, p.35.

[441] Ibid., p.36.

determination,[442] and Habeas Data rights implemented in many Latin American countries, which provide individuals with means to access data 'registries' with the ability to update, correct, or delete data.[443] Details of this will be discussed in Chapter VII, but it is important to note for now that the constitutional-level formulation of data privacy right as a 'freedom to' is a very important element of the regulatory mix[444] supporting PMM.

Secondly, implementing PMM is needed for the protection of public goods.[445] Public interest theories of regulation state that values like justice, redistribution,[446] social solidarity,[447] or preventing social subordination[448] are valid reasons for regulation. Privacy may be considered a value which fits in this list. More specifically, the collective level of privacy of all citizens underpins democratic institutions (as stated in Chapter III),[449] and privacy is a form of social control which is an internal dimension of society.[450] Therefore, all individuals have a common interest in preserving their autonomy regarding their personal data.[451] In this view, privacy is treated like freedom (or freedom of speech), which is an individual value, but also a collective one, because the prerequisite of free society is free individuals. So, citizens should recognise the importance of their own privacy and the privacy of others as important to society as a whole.[452]

Thirdly, the PMM model may be used to protect vulnerable groups.[453] Social anti-discrimination policies commonly include prevention of sexual, racial, ethnic or religious discrimination, as minorities may 'attract' social oppression. Those groups are more

---

[442] Which, however, is not written in the German Base Law. See Chapters II and VII.

[443] Guadamuz 2001, pp.5–6.

[444] Regulatory mix is understood as a set (mix) of regulatory tools.

[445] Cf Baldwin, Cave and Lodge 2012, p.22; Freiberg 2010, p.10; Bennett and Raab 2006, p.40; Ogus 2004, p.54.

[446] Morgan and Yeung 2007, p.26.

[447] Baldwin, Cave and Lodge 2012, p.22.

[448] Sunstein 1990, pp.61–64.

[449] Also, Schwartz 1999, pp.1647–1658.

[450] Solove 2007, p.763.

[451] Bennett and Raab 2006, p.40.

[452] Bennett and Raab 2006, p.44.

[453] Cf Sunstein 1990, pp.61–64.

vulnerable because lack of privacy may expose discrimination criteria. The types of data which can contain such criteria are in some jurisdictions more protected.[454] As discussed, profiling may expose discriminating factors either by reference to them or to some corollary traits. As a result, exposed groups may have no access to the same products and opportunities as other social groups. In this way, service providers may (even inadvertently) cause discrimination and perpetuate social inequalities. These are well known reasons which may support the broad-brush regulation mandating protection of those groups.

However, the online environment expose some groups in a particular way that is difficult to address with such broad-brush regulation because those groups are diverse. For example, this is a problem with a group of people having susceptibility to manipulation, as mentioned in Chapter III. They lack experience or skills to assess the commercial offers and, therefore, may be easily enticed into a fraud or a losing bargain. Lack of privacy of that group and easy access to them with ICT may expose them to harm in a way in which they are not exposed without using ICT. Another vulnerable group is people lacking technology skills. Lack of knowledge about the online environment may increase the risk and multiply the consequences of privacy breaches.[455] Furthermore, in addition to those groups, the privacy vulnerable may also be found among the better-off. Lack of privacy may expose their willingness to pay higher prices.[456] As their decisions have higher economic value, they may be more endangered by digital manipulation.[457] Additionally, it seems that a similar problem might be people whose private affairs may attract the attention of others.[458] Their privacy may be simply more valuable, as privacy breaches may attract more revenue from advertising. These considerations show that privacy distribution in society is not even and groups susceptible to privacy problems may be different than those impacted by uneven wealth distribution. These people may be found in virtually any social class, and it is difficult to devise legal rules addressing their protection.

---

[454] Eg GDPR, Article 9.

[455] Mossberger, Tolbert and Stansbury 2003, p.10.

[456] Strahilevitz 2013, p.18.

[457] The wealthiest in the world cover laptop cameras, Rogers 22 June 2016; also, there are particular frauds targeting executives, Gil 22 March 2017.

[458] Eg hacking celebrities, Garcia 27 September 2016.

Therefore, there is a place to argue for an effective privacy management tool making sure that protection is available for those who are vulnerable or feel vulnerable, regardless of their social class. PMM reinforces the position of such data subjects by enabling them to individually manage what data about them are revealed. Additionally, the support of a third party providing expertise on privacy may be adjusted to more individual criteria. This corresponds with findings of Bennett and Raab, who believe that potential social policy related to privacy is more likely to be based on equality of opportunities rather than equality of results.[459] By contrast, mandating certain level of privacy for whole groups of data subjects by, for example, preventing service providers from collection and use of particular types of personal data could be ineffective because it is difficult to define discrimination criteria in a 'profiled world'. It would also be seen as unnecessarily paternalistic[460] because overriding individual privacy preferences is a paternalistic restriction of freedom and responsibility. Similarly, paternalism would be a broad-brush regulation related to mandatory data sharing. Such initiatives aim at increasing personal data use 'for a public good' in a way which overrides data subjects' will by a 'social licence'.[461] However, paternalism resulting in 'oversharing' may be even more dangerous, as it ignores both individual and societal values of privacy.

2. *Correcting market failure*

PMM implementation can also strengthen data subjects' autonomy in the economic perspective remedying market problems. Under this argument, the goal of regulation is to reinforce the position of individuals as market players to restore the balance between parties. Baldwin and others recognise that the mere existence of unequal bargaining power may be considered as a per se reason for regulation.[462] However, more often the language of welfare economics and specifically the notion of 'market failure' is used as a rationale. As the market is considered an efficient tool to allocate resources, regulation is justified when an uncontrolled market fails to produce behaviour or results in accordance with public interest.[463]

---

[459] Bennett and Raab 2006, p.44.

[460] Solove 2013, p.1994.

[461] Cf Australian Government, Productivity Commission (No. 82) 2017, p.13; Data Futures Partnership 2017.

[462] As it prevents fair allocation of the resources, Baldwin, Cave and Lodge 2012, p.20.

[463] Ibid., p.15; Freiberg 2010, p.109.

The reasons may be related to non-compliance with important conditions for market theory: access to full information about goods, perfect competition, or the absence of externalities.[464] As the discussion in Chapter III shows, the online market for personal data is non-compliant with all these three conditions. PMM aims to preserve the market mechanism as the main tool for privacy bargains, and to introduce regulation only to help the market to operate.[465] This may be achieved by the means of addressing the problems detected in Chapter III related to asymmetries of information and power.[466]

Firstly, the PMM aims to provide data subjects with a mix of simple information[467] together with external expertise to overcome information asymmetry. Information asymmetries are a very important reason for market failure.[468] They make consumer choice imperfect because consumers do not have full information about the products and consequences of their choice. Privacy may be treated as a non-price element of the service received, an aspect of its quality.[469] The ability to distinguishing good quality service from a bad quality one is crucial for the market, because without such an ability good quality may be not available in the market at all.[470] Also, as noted in Chapter III, there may be little incentive for service providers to produce information or there may be even incentives to falsify or mislead customers.[471] Correcting this inefficiency may improve autonomous choice and market mechanisms.

---

[464] Ogus 2004, p.29.

[465] But, it also adjusts the domain of market to respect the inalienability of personal values protected by privacy.

[466] Cf with similar idea, "MyData" n.d.; also, Poikola, Kuikkaniemi and Kuittinen 2014; cf "Project VRM" n.d. which aims to re-organise relations between individuals and vendors to guarantee independence from those vendors; more in Searls 2012.

[467] See Chapter VI.

[468] Freiberg 2010, p.9; also, 'inadequacies', Baldwin, Cave and Lodge 2012, p.18; or, 'deficits', Ogus 2004, p.38.

[469] Stucke and Grunes 2016, p.119; Graef 2016, p.310; quality as multidimensional concept is described in OECD (DAF/COMP(2013)17) 2013, pp.5–6.

[470] According to a generalised Copernicus (Gresham) law bad quality may drive out a good one, Akerlof 1970, pp.488–490.

[471] Cf Baldwin, Cave and Lodge 2012, p.18.

However, the usual regulatory response to such asymmetry, obligation to disclose necessary information to consumers,[472] is imperfect. The reason for this, discussed in Chapter II, is known also as the 'transparency paradox'.[473] On the one hand, a comprehensive privacy statement (notice) is too detailed to be read by a regular user[474] while, on the other hand, simplified notice does not provide necessary information.[475] So, the information cannot be perfect, but should rather be optimal as to the relevant area of decision making (by customers).[476] In other words, disclosure needs to avoid the overload problem and be limited to a small amount of sensible and relevant information which gives the full picture.[477] This is the role of the organising function of PMM, which should provide simple overviews of data types and uses.[478] Also, third parties could support individuals with making decisions,[479] which should help to overcome the problems of disclosure regulation.[480]

Secondly, the PMM model gives data subjects direct influence on service providers' actions, which gives them similar control over their relationships as they would have if they were directly paying them (with money). In this way, data subjects could directly respond to the problems caused by the actions of service providers by withdrawing authorisation to use data or by deleting data. This is a method of ameliorating the effect of negative externalities recognised as a market problem. Negative externalities are a prominent reason for finding market failure,[481] and the rationale for regulation is to protect data subjects and society[482] from them. Those externalities are currently 'internalised' (ie their costs are brought into the

---

[472] Freiberg 2010, p.167.

[473] Nissenbaum 2011, p.36; also, Jones 2016, p.87.

[474] Which may also create a sort of 'safe haven' for businesses seeking to write marginal, but not outrageous terms, Hillman 2007, p.92.

[475] Similarly, in medical ethics it was found that the stricter the requirements for information the fewer people are covered by 'informed consent'. As a result, despite the best efforts to exercise individual autonomy, more people are regarded as lacking capacity to consent and treated on a paternalistic basis, Herring 2014, p.206.

[476] Freiberg 2010, p.24; Ogus 2004, p.40.

[477] Ben-Shahar and Schneider 2011, p.721.

[478] See Chapter VI.

[479] See Chapter V.

[480] Ben-Shahar and Schneider 2011, pp.746–747.

[481] Also, 'spillovers', Morgan and Yeung 2007, p.35; Freiberg 2010, p.8; Ogus 2004, p.32; Baldwin, Cave and Lodge 2012, p.18.

[482] Externalities may impact on common goods, Hardin 1968.

economic transaction) by either awarding individuals damages for the harm, or by excessive administrative fines paid by data controllers for infringement of statutory provisions.[483] Both of those methods are debatable. This is because it is difficult to recognise costs of harm to dignity or autonomy, and legal actions may prolong and aggravate this harm. Also, excessive administrative fines are only vaguely related to those costs and convert privacy enforcement into a specific 'hide and seek' game played between the service providers and DPAs in which avoiding fines is an end in itself.[484] In light of the ineffectiveness of these measures, PMM could provide data subjects with a simple market instrument in which they could monitor data transactions and react any time by withdrawing their authorisation and deleting their data. Furthermore, it may be argued that the risk of manipulation and coercion is decreased with PMM. This is because data are under control of data subjects and they can in any given moment verify and delete them.

Thirdly, a potential reason to implement PMM may be related to overcoming existing competition problems. As discussed in Chapter III, personal data markets have a tendency to produce huge companies which integrate vertically and occupy a large part of the global market. This can to some extent be remedied by introducing PMM, which should increase competitiveness in the market. This is because PMM reconstitutes a mechanism removed from some business models in which customers can 'vote with their feet' as a response to problems. PMM increases the buying power of consumers by balancing information asymmetries, increasing their control over their data, and reducing their dependence on particular service providers and their lock-in mechanism. The competition discussion is presented in more detail in the next chapter, which devises a set of measures to achieve these goals.

So, PMM implementation should strengthen the market competitiveness and may correct many of market failures. But, there are potential business opportunities for service providers arising from implementing this model.

[483] GDPR, Article 83.

[484] Cf 'goal displacement', Bamberger and Mulligan 2015, p.34.

3. *Oiling the wheels of digital economy*

The third argument in favour of PMM is that regulation by the means of PMM may be effective for service providers. The effectiveness of regulation includes also, as explained by Freiberg, "the extent to which it facilitates compliance and enforceability and has minimal adverse or unintended consequences."[485] Regulation by the means of PMM aims to facilitate interaction between data subjects and online service providers to create for both of them a safe environment where transaction costs are reduced.

In the case of service providers this may be achieved by eliminating problems which they are struggling with, and by changing the environment in a way which engenders trust between data subjects and service providers. Firstly, PMM resolves some major problems of the consent regime important for service providers. That is, it provides them with non-ambiguous legitimacy for data processing of different data which lowers the risk of non-compliance with current regimes. This risk currently arises because of the possibility of finding out that the consent was invalid, as it was not properly informed, blanket (ie the information provided was not specific enough), or even not freely given.[486] In other words, the ethical (and legal) underpinning of their businesses is weak which, in some cases, only waits to be revealed. This risk is serious not only because of hefty administrative fines,[487] or risk of further civil litigation,[488] but also because those data cannot be used to run a day-to-day business which breaks business continuity. PMM provides data subjects with the constant ability to make choices about their data, which gives businesses a strong argument that autonomous choice was made.

Also, PMM may give businesses a lot of flexibility in access to already collected personal data which may be used in new areas. This is because it could replace the existing mechanism of purpose limitation (or use limitation) governed by consent, which may be seen in the era of Big Data as obsolete.[489] Businesses planning new data use could simply let their customer

---

[485] Freiberg 2010, p.260 citing Robert A. Kagan.

[486] See Chapter II.

[487] Eg up to 4 per cent of global revenue, GDPR, Article 83.

[488] See GDPR Articles 79-82.

[489] Cate and Mayer-Schönberger 2013, p.72.

know that they are introducing a new option, and introduce it in parallel, as privacy settings are controlled by data subjects. This would substitute the usual procedure of collection of additional consent. Such a procedure in the electronic consent scenario usually requires specific disclosure and collection of proof of consent (together with the text of disclosure), but may be especially burdensome when current law requires written consent.[490] Therefore, PMM could be seen as a more elastic mechanism in extending data use, assuming that data subjects receive some benefit for such use.

Furthermore, deemphasising consent may make the process of entering into a contract more convenient for both parties. Convenience is very important for the economy, and this convenience is currently delivered by online contracts.[491] As identified in Chapter II, problems with regulations based on consent may be related to providing individuals with excessive amounts of information during the consent procedure. As disclosure (in T&Cs) is lengthy, the choice for businesses is either to present it to customers along with a mechanism for communicating consent (usually a sort of 'I Agree' button),[492] or to present the link to a separate page.[493] In either way it is unlikely that customers engage with the content of T&Cs. PMM could enable service providers to simplify disclosure of part of the consent procedure. It would make no sense to present the pages of disclosure if individual policies enforce customers' rules before entering the transaction. Also, customers knowing that their settings are enforced could be sure that services do not introduce unreasonable risk for them. Moreover, the existence of an individual privacy policy on a server of a third party acting for individuals would relieve them from the burden of constant consent requirements. This is because they could simply delegate the job of responding to these questions to technology and allow the automated system to adjust the online environment to *their* privacy requirements.

Secondly, PMM may give trustworthy service providers access to new data from existing and new customers. This could be done if PMM helps develop trust between the parties. Trust is

---

[490] Which is still the case in some European countries in data protection law, see Korff (ETD/2001/B5-3001/A/49) 2002, pp.26–27.

[491] Brownsword 2006, p.315; Kim 2013, p.27.

[492] In 'extreme' versions the customer is forced to scroll down the whole agreement until the 'I Agree' button activates.

[493] Cf. 'clickwraps' and 'browsewraps', Kim 2013, pp.39–42.

an essential component for an online relationship to be initiated and further developed.[494] From an economic perspective, trust is often understood as the creation of a predictable and relatively stable and reliable state of affairs or, in other words, as a method of creating social order.[495] So, economically-oriented researchers will often see that trust "oils the wheels of commerce"[496] by underpinning the contract mechanism and reducing transaction costs. This is because if people trust someone, the argument goes, they do not have to bear the costs of checking them, verifying all information, which may be very specialised and hard to assess. But, verifying information, a necessary component of a complex economy, requires dependence on experts, which cannot exist without a measure of trust.[497] Trust makes complicated transactions easier and allows the parties to concentrate their efforts on their goals. In a wider view, trust underpins relations, bounds community, and forms 'social capital'.[498] These are the reasons why the topic of trust is almost omnipresent in the privacy debate. [499] It can be seen in policy documents of the economic organisations which state that trust is vital,[500] and 'digital trust' need to be strengthened.[501] It can be seen in statements about the need for trust raised by businesses,[502] consultants,[503] competition authorities,[504] in standards,[505] and in the motives for regulation.[506] Businesses building e-commerce want to know how to present themselves to their customers as safe and trustworthy.[507] In sum, digital trust is of utmost importance for the business.

---

[494] Laurie 2002, pp.6–10.

[495] Freiberg 2010, p.13; also Fukuyama 1995; and O'Neill ("Reith Lectures") 2002.

[496] Bennett and Raab 2006, p.51; the expression comes from Goff 1984, p.391.

[497] Frankel 2001, p.463.

[498] "A capability that arises from the prevalence of trust in a society or in certain parts of it", Fukuyama 1995, p.26; also, Putnam 1993; Nissenbaum 2001.

[499] Bennett and Raab 2006, p.52.

[500] OECD Guidelines 2013, p.95.

[501] World Economic Forum 2012; OECD ("Digital Economy Ministerial Meeting") 2016.

[502] Orange and Loudhouse 2014.

[503] Accenture 2016.

[504] House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.12.

[505] ISO/IEC 29100:2011, p.vi.

[506] GDPR, recital 7.

[507] Eg Beatty, Reay, Dick and Miller 2011; or Wang and Emurian 2005; Barney and Hansen 1994; Golbeck 2009.

But, trust is also a very complicated set of ideas on which researchers rarely agree. It may be understood as confidence in the reliability and safety of the existing privacy framework.[508] Furthermore, trust is dynamic and builds in situations of repetitive interactions.[509] It develops, builds, declines, or even resurfaces in the course of the relationship.[510] Trust "grows out of active inquiry" by observing how well claims and undertakings to act hold up.[511] Regulation cannot coerce service providers into being reliable, but may increase transparency of their actions, and increase the value of their reputation by setting up a clear system of rewards and punishments for betrayal of trust. It can also decrease the risks of individuals, especially when they are entering relationships with online service providers.

PMM may help in many of those goals by increasing visibility of service providers' actions. The controlling function of PMM aims to provide data subjects with monitoring of their data, so they could base their decisions about trustworthiness of service providers on facts. In addition, third parties involved in data monitoring may provide some additional information.[512] This creates an environment in which evidence of good relationships with a company may be used to make decisions for the future. It also creates an environment in which dishonesty is detected.[513] Such an accountability mechanism would help to develop trustworthiness,[514] and help to make service providers incentives more synchronised with the incentives of data subjects. Furthermore, PMM would make it easier to make the first decision to trust and enter into an online relationship, because data subjects would know that regardless of the T&Cs their privacy settings have precedence over them, and, they would know that they could withdraw from such a relationship in any moment, taking their data with them. These features decrease the risks of individuals by working as a 'safety net' for those whose trust is

[508] Eg trust is explained as relying on the elements of OECD Privacy Framework's principles in OECD Guidelines 2013, p.95.

[509] Cf the idea that cooperation is possible where choices of cooperating parties determine their future actions, Axelrod 1984, p.12.

[510] Rousseau and others 1998, p.395.

[511] O'Neill ("Reith Lectures") 2002.

[512] Cf the role of 'third party inspection', The Federal Trade Commission 2016, p.31.

[513] More broadly about the costs of dishonesty, Akerlof 1970, pp.495–496.

[514] Cf the view about facilitating the formation of bargaining institutions to enabling the cyberspace to evolve, Easterbrook 1996, pp.215–216.

betrayed.[515] This is especially important on the Internet, where verification costs are higher (due to the lack of direct communication),[516] and for new market entrants.[517] Thus, by creating an environment in which customers are put first, PMM may be a good tool to convince existing customers of trustworthy service providers to share more data and attract new ones.[518]

Developing trustworthiness in the way described above is tantamount to building a framework of accountability. The concept of accountability may be seen as amorphous,[519] and capable of substituting 'responsibility' or 'liability' for data controllers' actions by 'reinventing' self-regulation in a new guise.[520] So, it needs to be explained in the context of PMM. The main idea behind accountability is that data controllers (service providers) should have in place appropriate measures of privacy management and be prepared to *demonstrate* compliance to those measures (and/or to verify how these measures are implemented).[521] In this sense, it goes beyond responsibility as it obligates service providers to be answerable (called 'to account') for their actions to an external agent.[522] And, it implies some interaction in which this external agent seeks answers and rectification.[523]

PMM could be seen as providing this accountability-enabling interaction to the external agents who are data subjects. Many descriptions of accountability in respect of privacy protection do not specify to whom data controllers should be accountable.[524] The external agent could be a Data Protection Authority (DPA) or some other "external stakeholder",[525] presumed to have

---

[515] Cf Nissenbaum 2001, p.646.

[516] Frankel 2001, p.459.

[517] Incumbent companies like Facebook or Google already have a huge customer bases.

[518] Giving control to customer may be a powerful strategy, Detlev Zwick and Nikhilesh Dholakia 2004, p.40; cf finding 3.1 of Australian Government, Productivity Commission (No. 82) 2017, p.33.

[519] Alhadeff and others 2011, p.27.

[520] Bennett 2012, pp.40–43; Raab 2012, p.16.

[521] See ss 14 and 15 of OECD Guidelines 2013; s 5.10 of ISO/IEC 29100:2011; Article 29 WP (WP 173) 2010, p.3; GDPR, Article 5(2); Le Métayer 2016, p.427.

[522] Bennett 2010, p.3; Centre for Information Policy Leadership 2009, p.11; Papanikolaou and Pearson 2013, p.2.

[523] Bennett 2010, p.3.

[524] Asia Pacific Economic Cooperation ("Privacy Framework") 2005, p.28; OECD Guidelines 2013, p.16; ISO/IEC 29100:2011, p.18; also, discussion in Bennett 2010, pp.4–6.

[525] Footnote 1 in Article 29 WP (WP 173) 2010, p.3.

some rights of authority over those accountable and possibility of external compulsion to change practices related to data.[526] Some authors seem to recognise that data subjects themselves are the ones to whom data holders should be accountable and give necessary tools providing transparency of information use and ability to take actions guaranteeing compliance.[527] A similar idea seems to be included in a discussion paper of the Centre for Information Policy Leadership which recognises among essential elements of accountability the mechanisms of individual participation.[528] This is an approach consistent with PMM which puts individuals in the driver's seat. Furthermore, PMM gives the highest level of accountability, accountability of practice.[529] A predominant number of organisations are accountable on the level of policy,[530] some of them are accountable with respect to particular procedures, but very few subject themselves to verification of practice. As Le Métayer explains, the first type of accountability is purely declarative, the second adds organisational measures, and only the third applies to actual actions.[531] This is because data subjects cannot check the accountability of T&Cs,[532] nor verify internal privacy incident (or data security) procedures,[533] but in PMM they can verify what is being done to their data. In this way, service providers' accountability may be exchanged for data subjects' authorisation for data transactions.[534]

In such a way PMM aims to provide individuals with control over data without disruption to existing business models and at a lowest possible costs. That is to say, personal data remain available for them but could be used only according to data subjects' privacy policies.[535]

---

[526] Bennett 2010, p.3.

[527] Weitzner and others 2008, pp.84–87.

[528] Centre for Information Policy Leadership 2009, pp.13–14. This idea is somewhat unexpected in this document, which otherwise seems to aim at a low level of accountability comparing to eg ISO/IEC 29100:2011 or Article 29 WP (WP 173) 2010.

[529] Cf Bennett 2010, pp.6–7.

[530] Ie they have a policy.

[531] Le Métayer 2016, p.427.

[532] They can read it, but, as will be shown in Chapter VII, it does not bring much value because of their vagueness and changeability.

[533] Which still can be done by DPAs.

[534] Cf Bennett and Raab 2006, p.227.

[535] See more in the next chapter.

Building interfaces for PMM and their maintenance is, of course, and additional cost for service providers, but there are potential savings on implementations of differing (across societies and countries) policy options which in this model is left for users and third parties who support them. That is to say, with the use of PMM, global services could be more easily adapted to differing perceptions of privacy and regulatory obligations.[536] Furthermore, as will be shown in Chapter VI the functionality of technical interfaces is an extension of existing privacy tools already used by service providers. Overall, these are not major burdens for bigger service providers which would be targeted by such regulation. Although it may be claimed that they could end up with fewer customers, that risk should be manageable because PMM works mainly through accountability. So, if what they do with personal data is 'palatable' to data subjects there should be no problem with providing them with tool exercising autonomy.

So, PMM may be seen as a tool which "oils the wheels of commerce", because it eliminates concerns which should be important for service providers, and creates an environment of trust between them and data subjects. It removes business risks related to legitimacy for data processing and provides business with flexibility in repurposing already collected personal data for the new areas of use. Also, PMM could give the trustworthy service providers a way to access new data from existing and new customers. Trust in this model is engendered by increasing visibility of service providers' actions and creating an environment in which dishonesty is detected and evidence of good relationships may be used to make subsequent decisions about data use. Furthermore, PMM decreases the risk of entering into a contract with the online service provider by working as a 'safety net' for those whose trust may be betrayed. It may be also seen as the best accountability mechanism – accountability of practice.

All these arguments show that regulation by the means of PMM is needed. But, what regulatory tools need to be applied to regulate for PMM? And, which privacy regime is able to ensure its implementation?

[536] See Part C below and the following chapters.

C What is Needed to Regulate for Privacy Management?

Knowing that PMM is the right plan to overcome the detected problems is not enough, because it needs to be implemented with adequate regulatory 'tools' and by the actors which have the potential to do it successfully. In this respect, even a cursory look at PMM shows that traditional legal regulation is not enough to implement it. This is because it requires specific measures of control, such as interfaces in ICT systems, and because it requires a 'business model' in which individuals get support from third parties. In other words, it requires hybrid regulatory tools (methods).[537] Also, those tools are interdependent and may create synergies or conflicts.[538] Furthermore, the tools need to be used by particular regulators within the context of the institutions of existing regulatory regimes. The regulation of online services is polycentric and pluralist. There are many regulating entities (actors) on different levels (national, international) and their efforts meet in a common 'regulatory space'.[539] So, to put PMM in this space, there is a need to find the best regulating actor and devise for such an actor a mix of regulatory tools. The discussion below shows how this can be done.

1. *Which regulatory tools are needed to implement Privacy Management?*

As outlined earlier, regulating cyberspace requires a wide portfolio of tools as a varied toolbox brings better, more tailored regulation.[540] Setting out these measures to implement PMM starts from Lessig's model of four constraints (or 'modalities') of individual behaviour: law, the

[537] Raab and De Hert 2008, p.274; Black 2001, pp.105–112; cf the drawbacks of purely legal approach in Bamberger and Mulligan 2015, p.34.

[538] Raab and De Hert 2008, p.271.

[539] Raab and De Hert 2008, p.274; Freiberg 2010, pp.18–19.

[540] Cf Gunningham, Grabosky and Sinclair 1998, p.4.

'code'[541] (or architecture), norms (or self-regulation) and market forces.[542] They are shown in Figure 14:[543]

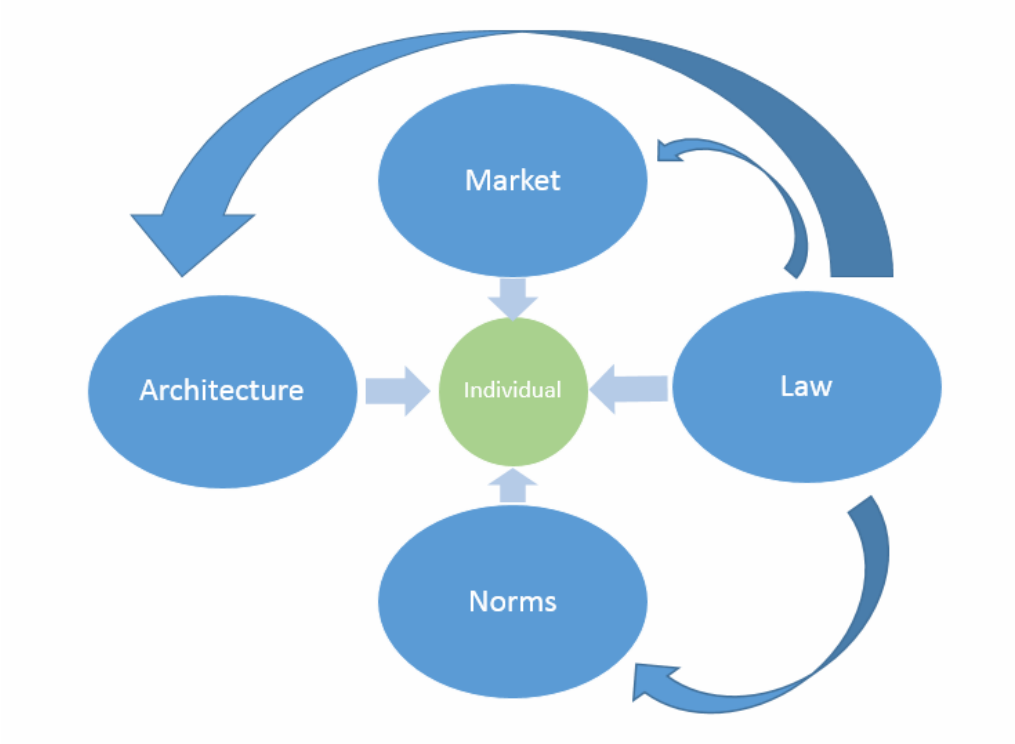


Figure 14 Lessig's four modalities (regulating forces)

As presented in Figure 14 (which is taken from Lessig's own work), in this approach the regulatory mechanisms are understood broadly as actions influencing the subjects directly or indirectly through other 'modalities'. The first of these modalities, law, includes all legal tools which influence individuals and other modalities. Norms are social rules enforced by other members of the community. People conform to them as they are afraid of social sanctions. Then, market forces work by means of economic incentives, which are usually based on pricing. Finally, architecture (or 'code') implements constraints on behaviour or choices by the very structure of the virtual world – hardware and software.[544] The overall regulatory approach is to design an 'optimal mix' of those modalities.[545]

---

[541] It means a computer program executed in a computer architecture. The distinctiveness of this environment was most famously announced by David Clark, one of the main Internet architects in 1980s: "We reject: kings, presidents and voting. We believe in rough consensus and running code", Clark 1992, p.19.

[542] Lessig ("The Law of the Horse: What Cyber Law Might Teach") 1999, p.507; Lessig ("The Architecture of Privacy") 1999, pp.62–63. An individual is understood here as any subject, so also service provider.

[543] Lessig 2006, p.125.

[544] Lessig 2006, p.124.

[545] Lessig ("The Law of the Horse: What Cyber Law Might Teach") 1999, p.513.

The Lessig approach remains very influential. In particular, the idea of 'code' has been adopted by many other authors.[546] Of all the models seeking to regulate 'cyberspace',[547] this remains the best place to start because of the way it emphasises the role of technology, which constructs the world in which the privacy problems arise and constrains what actors can and cannot do there. As demonstrated in Chapter III, online privacy problems arise because technology (architecture) deprives data subjects of choices relating to their data. Therefore, regulation tackling these problems needs to recognise the role of technology[548] and use its tools to enable data subjects to have those choices. Experience shows that the 'code', if ignored or neglected, can exploit weaknesses in the law.[549] But, the 'code' can be shaped by the law. Furthermore, it is "incredibly malleable", because it is not bound by the rules of the physical world.[550] Therefore, it is a basic tool to create norms in an online environment, enforce them,[551] limit and transform any legal actions corresponding to 'virtual world'.[552]

Nevertheless, the Lessig model has its limitations and it should be applied with a dynamic view of its modalities taking into account social and political processes.[553] Also, any view of the technology should be as devoid as possible of political agendas.[554] But, in spite of its simplifications, Lessig's theory still forms a good starting point for thinking about the regulation of technology. So, how can those modalities be used to implement PMM?

---

[546] Cf design-based instruments, Yeung 2008, p.79; technological instruments, Bennett and Raab 2006; design solutions, Baldwin, Cave and Lodge 2012, p.122; structural regulation, Freiberg 2010, pp.158–165; ambient regulation, Hildebrandt 2008; normative technology, Koops 2008, p.158.

[547] Eg nodality, authority, treasure, and organisation by Hood and Margetts 2007, p.5; taxonomy of regulatory strategies in Baldwin, Cave and Lodge 2012, pp.105–130.

[548] Cf Kirby 2008, p.382.

[549] Eg the case of copyright, Giblin 2011, p.4.

[550] Giblin 2011, p.8.

[551] Koops 2008, p.161.

[552] More about the shortcomings of addressing ICT problems by the means of law built on assumptions from the 'real' world, Giblin 2012.

[553] Raab and De Hert 2008, p.282; also, Gutwirth, De Hert and De Sutter 2008, pp.194–196; Rowland, Kohl and Charlesworth 2017, pp.14–15.

[554] Gutwirth, De Hert and De Sutter 2008, p.215; similar argument seems to be the strongest in the conclusions of Mayer-Schonberger 2008, pp.745–746.

(a) Market (or economic regulation)

The first modality, the market, refers to an economic mechanism which influences individuals by making some of their actions more or less available. The main driver here is economic efficiency. This is usually measured in money by the means of a cost-benefit analysis which provides individuals with incentives to act. As described in the previous chapter, personal data have an economic value derived from the prospect of future income earned with their support. Having such value they are traded on 'data markets'. Therefore, economic regulation should find a counterbalance for market power of service providers and their incentives to earn on data. 'Data markets' as other types of markets can be stimulated by incentives or information, harnessed by, for example, competition law, or influenced by nudges, or direct deployment of wealth: contract, grants, loans, or subsidies.[555] Markets can also be created, as proposed by Laudon in his influential paper *Markets and Privacy*.[556] The next chapter will show how PMM could operate in the context of the 'data markets' and how those markets can be influenced to create a more balanced environment. But, markets do not exist in a vacuum, they are always constituted by law and norms – cultural elements related to the behaviour of market participants.[557]

(b) Norms

Norms refer to the internal (to society or industry) norms enforced by other members of a community. This includes all approaches to regulating privacy through self-imposed obligations which are usually non-binding. Sometimes the limits of norms as a tool are vague, as self-regulation may be enforced by government, may have the form of co-regulations, or

[555] Baldwin, Cave and Lodge 2012, pp.111–126.

[556] He proposed recognition of property interest in personal information and creation of government controlled National Information Market, Laudon 1996, p.99; a similar proposal to assign property rights (but also to let the market forces to operate) was put forward in Lessig 1999a, p.520; they were criticised for initial inequality, Nissenbaum 2009, p.79; and, Cohen 2000, p.1390; also, for problems in assigning rights to information, Samuelson 2000; and, for structural problems and encouraging privacy violations, Schwartz ("Beyond Lessig's Code for Internet privacy: Cyberspace filters, privacy control, and fair information practices") 2000, pp.763–771; Schwartz 2004, p.2111.

[557] Freiberg 2010, pp.130–131.

even meta-regulation (where government oversees the risk management process).[558] There have been many approaches to self-regulation in data privacy and they will be discussed in the following chapters along with other 'modalities'. They have all been ineffective, which suggests that this tool should be less important. However, those self-imposed obligations are very important to show the bottom line of what businesses can willingly deliver, and what tools are considered by them as the most appropriate (probably cost-optimal).

(c) The 'code' (architecture)

As mentioned, it was widely acknowledged that the 'code' is of special importance in the regulation of online services. It is important to set out here exactly what the 'code' means and how it may be harnessed to implement PMM.

The 'code' (architecture or design techniques) is a method of influencing behaviour through the design of physical or logical structures of ICT systems, which remove or limit choices by enabling or disabling certain actions.[559] It consists of software, hardware, and also network protocols.[560] In fact, it could include any kind of technical components, as the internal elements of ICT systems are to some extent equivalent[561] and organised in a way to fulfil their business role.[562] Furthermore, there is no clear distinction between technology understood narrowly and the broader meaning of technology as organisational structures and processes surrounding the computer systems.[563] Therefore, in this thesis, technology is conceived of broadly[564] as there

[558] Baldwin, Cave and Lodge 2012, p.147; Freiberg 2010, pp.33–37.

[559] Lessig ("The Law of the Horse: What Cyber Law Might Teach") 1999, p.519; the first full expression of this idea was known as 'Lex Informatica', Reidenberg 1998, p.568; some preliminary thoughts can be found in Lessig 1996, pp.896–898; the sentence "code is law" was first written by Mitchell 1995, p.112; however, origins of this are most probably in remarks about the networks of exercising power in the fields of knowledge or technology in Foucault 2000, p.123.

[560] Greenleaf 1998, p.606.

[561] Ie to some extent logical functionality of software can be implemented in hardware, or distributed system may be arranged as a centralised one.

[562] Cf with Giblin who was of the opinion that only software has the specific features of 'the code' Giblin 2011, p.7.

[563] Bennett and Raab 2006, p.178.

[564] According to Merriam-Webster Dictionary, technology may be understood as "a manner of accomplishing a task especially using technical processes, methods, or knowledge".

is a need to think about whole ICT systems and no real way to get insight into complicated structures comprising software and hardware elements organised into the processes of providing Internet services.[565]

The 'code' acts in a manner which, in fact, determines rights and obligations of the parties, so as an equivalent of the law, hence the sentence: "the code is the law".[566] This is, to some extent nothing new, for example, nowadays there are probably no cars without seatbelts, most countries limit access to firearms, treat drinking water, or shape city architecture to modify human behaviour. But, the 'code' is more pervasive as it acts immediately by defining what is 'visible' and possible in the ICT system. It can provide the data subjects with opportunities to make decisions, or invisibly steer them away. In this way, people experience control as a natural order of things.[567] What is allowed is visible and accessible; what is disallowed simply does not happen. There is no disobedience against regulation by the 'code'. Furthermore, the 'code' can be changed 'on the fly' as in the case of "tethered appliances" – devices remotely connected to their manufacturers or vendors which automatically install or alter the code.[568] When it is changed, in the twinkling of an eye people are given different set of choices, and what was before exists no more. The only option system users retain is the ability to decline to use the system at all, which may not be possible or practicable. This is a perfect system of regulation by itself.

Furthermore, it is a system to some extent detached from law. Of course, law may (or should) influence the creators of the 'code'. But, there are no moral or legal presumption of the operations of the 'code'.[569] It can change the outcome of legal regulation or even displace the law because the system architects did not provide users with certain options.[570] As a result, its

[565] These complexities will be hidden. As a result of broader approach, the 'code' might be slightly less malleable than code which is purely a software one.

[566] Lessig 2006.

[567] Lessig 2006, p.138.

[568] Zittrain 2008, p.132.

[569] Code is neither inherently privacy invasive nor enhancing. It simply reflects the values of writers and owners, Edwards 2004, p.16.

[570] Laws have limited power to regulate the cyber world, especially if they face the 'anti-regulatory' code, Giblin 2011, p.4.

legitimacy may be questionable,[571] as its operation may be not based on the rule of law,[572] but rather on the concept of T&Cs' violation.[573] Furthermore, such regulations may still generate errors (eg block some permissible behaviour or not block impermissible behaviour), but it is harder to monitor, find and assess them.[574] However, the way the 'code' interacts with user behaviour may also be much more nuanced. Technology may design-out the non-compliance, but may also only discourage it, or improve the chances of detection.[575] In fact, in regard to the relationship between service providers and data subjects, it may work on a few more levels, as presented in Table 3.[576]

Table 3 Different levels of the influence of the 'code'

Type of influence	Influencing data subjects	Influencing service providers
Informational	Give access to information / visibility of data actions	Provide data subjects with information / visibility of data actions
Neutral	Give tools to make decisions	Provide data subjects with tools to make decisions
'Liberal paternalism'[577]	Discourage data communication	Discourage data processing
Partial paternalism	Restrict data communication	Restrict data processing
Full paternalism	Design-out personal data communication to service providers	Design-in privacy protection excluding personal data processing

As described above and for the reasons stated there, PMM aims to provide only informational and neutral influence (marked green in the table). That is to say, it aims to offer a mechanism of informed choice located in a neutral environment.[578] This implies the use of certain technological tools which rather than designing privacy protection into the very mechanism

[571] Yeung 2008, p.80.

[572] Zittrain 2008, p.140.

[573] Zittrain 2010, p.1772.

[574] McIntyre and Scott 2008, pp.116–119.

[575] Brownsword 2008, p.39.

[576] This is just one vision of such interaction and other views may exist.

[577] A mixed liberal and paternalistic system, Thaler and Sunstein 2009.

[578] Cf the postulate of preserving capacity for genuine choice, Brownsword 2008, p.42.

of ICT systems are aimed at the facilitation of choice and data management. This also imposes certain legal mechanisms necessary to shape those technological tools.

Such a system may be globally universal, but it also leaves room for policy decisions in countries that would like to shape their laws with some paternalism for any reasons. Having the mechanisms of choice implemented by the service providers, it is possible to implement different flavours of paternalism in a way the objective expectations of privacy are applied through external privacy interfaces. This depends on the business model or, more widely, on the role of third parties in this system. More specifically, a fully liberal approach[579] could be exercised by allowing individuals to freely choose the third parties operating in a business model guaranteeing competition between them and independence from service providers. 'Liberal paternalism' could be achieved, for example, by using 'nudges' to shape individuals' approach to privacy settings either directly or through those third parties.[580] Further levels of paternalism may be achieved by limiting choice as to the third parties (eg by some mechanisms of certification) and as to the particular privacy settings (eg forbidding some of them). At the end of this continuum is probably the state-owned 'platform for privacy settings' where individuals have little choice as to their own settings. This vision may be not acceptable for most readers, but, at the end of the day, authorities in such countries need to face their own citizens.[581] Despite this complexity and different policy approaches, global online service providers could have just one set of interfaces which could be used globally for privacy settings. This would probably be a cost effective way of implementing diverging privacy requirements from different parts of the world.

(d) The fourth modality: Law

The last of the regulatory tools, law is used to directly shape behaviour of parties and to shape other tools of regulation. There is a need to narrow down the scope of legal tools to those able to cover the privacy problem: data privacy laws and data privacy rights. As most countries in

[579] Which is encouraged by the author.

[580] More in Thaler and Sunstein 2009.

[581] And, the purpose of this thesis is not to convince to liberal democracy, but to design a model for widest possible use.

the world nowadays have omnibus data privacy laws[582] covering activities related to processing of personal data, they will be naturally the focal point of the legal part of this thesis (Chapter VII). Also, the personal value of privacy is protected in many countries by privacy rights. As mentioned in Part B above, they are very important to the proposed solution. This is because they act as a common point of reference and support to data privacy laws. They are, of course, not absolute and can be balanced against other rights which may protect the personal or economic values of others or the public interest.

Other branches of law will be considered only incidentally. For example, the lens of competition law will provide help to understand market in the next chapter, but, as will be seen there, competition law cannot provide a solution. This is because competition law and consumer (protection) law may protect only the interests of individuals as consumers or market participants. Consumer law application is considerably broad and protects consumers from deception and other unfair practices which may be related to personal data. Competition law often applies differently to different firms depending on their market positions and personal data may be an important asset of market participants. But, neither consumer nor competition law aims principally at protection of privacy values. They end up when the competition is protected and consumers' interests are safe, but they may not achieve informational autonomy or effective privacy management.

Similarly, the contract law by itself does not have its own solutions to take into account privacy implications. As discussed in the previous Part, this thesis aims to preserve as much as possible the underlying mechanism of contract law, as private ordering is an important mechanism of distribution in a liberal society. Having said that, this mechanism in the case of online services should be limited. This is because contracts where data are passed as consideration are fully dependent on the T&Cs imposed by a drafting party, which, furthermore are subject to unilateral changes, and used in a goal to appropriate personal data.[583] Enough evidence has been given in this thesis to justify limitation of the freedom of contracts (eg imbalance of power, information asymmetry, lack of autonomy, externalities),[584] and to say that in online

[582] Greenleaf 2014.

[583] Kim 2013, p.52.

[584] Eg Trebilcock 1993.

services the traditional picture of a contract as a 'meeting of minds' is gone.[585] It is autonomy which is supposed to be a fundament of liberal society and market economy,[586] and not the other way around. Such a reversed ramification would be a mistake. In contract law, all the ways to take into account the legitimate interest of the other party go towards incorporating societal standards: good faith,[587] fair dealing, or reasonableness. But, privacy is very subjective and should not be boiled down to societal standards. It is hard to speak about reasonable expectations of parties who do not (and even cannot) know the terms of the contract. Furthermore, the problem with online contracts is that they *create* the reasonable expectations of privacy via the commonly acceptable practice of big companies and, then, shift this norm.[588] So, the intervention into freedom of contract is needed and it needs to be done from outside of contract law.

However, this poses a question about proportionality of such intervention into contract law by the means of PMM. Assuming that regulation is justified and necessary, does the use of PMM prevent parties from making privacy deals which would be desirable for them? The starting point to this analysis is that data subjects could always exercise control over their data through PMM interface. So, PMM would surely prevent data subjects from selling out their personal data without possibility of taking them back.[589] But, the deals which require access to personal data for a specific period of time, for example, access to health data for the sake of providing health services would still be possible and left for the parties to decide. As data subjects would be able to withdraw data and change privacy settings any time, the online contract should foresee such an option. Intervention by the means of PMM may be seen as the extension of Brownsword's idea of duality of consent, which relies, first, on choosing a particular body of rules to govern dealings, and, second, on accepting particular transactions.[590] In such a case there is a need to limit consent in this first meaning by providing a set of rules to govern the

[585] Radin 2007, p.196.

[586] Trebilcock 1993, p.8.

[587] If such a general principle exists. For example, in English law it does not, Brownsword 2006, p.115 ff.

[588] Eg Kim 2013, pp.74, 87.

[589] Justification for this is inalienability of personal data. As a reminder, only data processing based on private interest is discussed here.

[590] Brownsword 2006, p.294.

dealings.[591] In other words, PMM regulates through setting 'the rules of the road' to help participants in online transactions.

Also, an additional limitation to contract is needed which prevents binding personal data processing with some contract terms. This is because PMM would be a useless tool when, for example, provision of service could be conditioned by collection of all types of data as an 'all or nothing' choice. Such limitations have already been enacted in some countries. For example, the European General Data Protection Regulation enables data subjects to withdraw consent any time,[592] and it makes some steps against binding providing the service with the consent to collection of data not necessary to perform this service.[593] Also, this may help to respond to the problem of the "unravelling effect" described by Peppet, turn of the economy towards voluntary disclosure (which is seen mainly in the insurance market).[594] This is because PMM could provide an environment in which individuals have accurate information about what is shared and with whom. So, most of the problems of such disclosure relating to data inaccuracy, lack of access, and (possible) oversharing[595] could be avoided,[596] and the only remaining problem would be whether the data required by service providers are necessary to perform a contract.[597]

In conclusion, to describe PMM implementation this thesis considers the Lessig model of four 'modalities' of user's behaviour: law, the 'code' (or architecture), norms (or self-regulation) and market forces. Market, or economic regulations will be further analysed to find a way to restore the balance of power in online services and to present a 'business model' of PMM service. Norms as self-imposed obligations will be analysed along with other tools to show what businesses could deliver by themselves and what solutions they consider as the most

---

[591] This may be better recognised in continental legal systems where "a body of rules to govern the dealings" comes into transaction as a civil code's "default" terms from which some are limited (*ius semidispositivum*). Therefore, all contracts are "naturally" limited.

[592] GDPR, Article 7(3) and recital 42.

[593] In such cases, consent may be seen as not freely given, so invalid, GDPR Article 7(4) and recital 43.

[594] Peppet 2011, p.1156; also, The Norwegian Data Protection Authority ("It's getting personal") 2017, pp.3–8.

[595] Also, inability to check how data are used causes increasing speculations about abusing them, eg Chowdhry 7 June 2016; or, Le Nouaille 25 August 2017.

[596] Cf Peppet 2011, pp.1177–1180.

[597] Cf The Norwegian Data Protection Authority ("It's getting personal") 2017, pp.6–8.

appropriate. The 'code' as a method of influencing by designing-in or removing choices in ICT systems will be analysed only to the extent to which it can provide data subjects with a mechanism of informed choice and tools to manage data. The last of the regulatory tools, law, is used to directly shape behaviour of parties and to shape other tools of regulation. This thesis will be interested only in the legal tools able to cover privacy problems: data privacy laws and data privacy rights. They limit to some extent the freedom of contract, but this is needed to provide the set of rules to govern the dealings ('the rules of the road') and create a frame of a safe and predictable contract environment for participants in online transactions.

As the scope of regulatory tools has been outlined, it is time to describe who should use them.

2. *Which regulatory regime should implement PMM?*

Privacy regimes include actors interacting on different levels and exerting to various degrees their influence on different regulatory tools.[598] So, it is important to propose a solution which balances their interests as its practical implementation depends on some level of compromise of the main stakeholders. As discussed above, there are reasons to think that PMM is such a solution. However, the market players may not be able to introduce PMM by themselves.[599] It should be specified by some regulatory regime either at national level (of particular states) or international level (of an organisation of states). Which one to choose?

Although national states are not the only source of regulation in the online environment, they remain very important as the main source of laws. But, their role is in practice diminishing.[600] The rise of the Internet created the underlying global infrastructure to distribute information and also to distribute power.[601] This infrastructure is very loosely controlled by most states[602] and may even redefine their role as mere providers of identity services enabling residency, doing business, or having bank accounts. For example, Estonia implemented an e-Residency

[598] Called a 'post-regulatory state' in Scott 2005; also, a simpler view of indirect regulation in Black 2001.

[599] This will be discussed in the next chapter.

[600] Although, as stated by Murray, it is too early to claim the existence of the 'Cyberstate', Murray 2008, pp.297–298.

[601] Cf Foucault 2000, p.123.

[602] Although, the Snowden revelations show new means for exerting such control.

program encouraging entrepreneurs to conduct their businesses through (or virtually from) Estonia.[603] This shows how in the global network states may compete to attract residents paying taxes. States may also be pushed out of the networks distributing information,[604] money,[605] and power.[606] So, many countries, especially smaller ones, are not able to regulate online services and they do not even try to. For example, in New Zealand the online services provided from abroad are governed by the laws of other jurisdictions.[607] This should pose some difficult questions as to the role of the state in regard to its residents. For example, Brownsword explains that the state has the responsibility to protect conditions constitutive of individual agency and a meaningful community.[608] But, how would it be possible to intervene when provision of Internet services is out of jurisdiction? The natural idea would be to regulate online services in the jurisdiction where they are located.

It is easy to find out that this jurisdiction is the United States. The best overview of the online market gives the index of the global Internet companies in 2017 ordered by market capitalisation:[609]

[603] They can apply online and receive the status of e-Residents without leaving their 'own' countries, 'e-Residency - e-Estonia' n.d.

[604] The Internet.

[605] Cf the rise of the alternative monetary mechanisms (e-currencies).

[606] Some countries already recognise that significant power comes from technology owners, see Baugh 2017.

[607] Law Commission August 2010, p.390. Details in Chapter VII.

[608] Brownsword 2008, p.46.

[609] Kleiner Perkins Caufield Byers 2017, p.322.

Rank	Company	Region	Current Market Value ($B)
1	Apple	USA	$801
2	Google - Alphabet	USA	680
3	Amazon	USA	476
4	Facebook	USA	441
5	Tencent	China	335
6	Alibaba	China	314
7	Priceline	USA	92
8	Uber	USA	70
9	Netflix	USA	70
10	Baidu	China	66
11	Salesforce	USA	65
12	Paypal	USA	61
13	Ant Financial	China	60
14	JD.com	China	58
15	Didi Kuaidi	China	50
16	Yahoo!	USA	49
17	Xiaomi	China	46
18	eBay	USA	38
19	Airbnb	USA	31
20	Yahoo! Japan	Japan	26
Total			$3,827

KLEINER PERKINS

Source: CapIQ, CB Insights, Wall Street Journal, media reports. Market value data as of 5/26/17.
Note: For public companies, colors denote current market value relative to Y/Y market value. Green = higher. Red = lower. Yellow = private companies, where market value represents latest publicly announced valuation. Ant Financial and Didi Kuaidi valuation per latest media reports as of 6/16 and 4/17 respectively. Xiaomi valuation per latest media reports as of 4/17. Ant Financial treated separately from Alibaba as Alibaba retains no control of Ant and will receive a capped lump sum payment in the event of an Ant liquidity event. Cash includes cash and equivalents and short-term marketable securities plus long-term marketable securities where deemed liquid.

KP INTERNET TRENDS 2017 | PAGE 322

Figure 15 Market capitalisation of global Internet companies in 2017, according to KPCB

It is clear that American and Chinese companies dominate the list. As Chinese companies operate mainly in China, the rest of the world is left to American supremacy, and, the first four US companies from Figure 15 above together with Microsoft form the top five biggest firms in the world.[610] The United States is also the biggest exporter of online services. This has an important influence on any potential regulatory activity towards this industry, because service providers are located in another jurisdiction than those researched in this thesis, while their operations undoubtedly have effect outside the US.

In theory, the privacy aspect of online services should be regulated by US laws,[611] but it is unlikely to happen. Despite the early adoption of privacy rules for public services (Privacy Act 1974) those laws have not been further developed at a federal level to data privacy in relation between private entities.[612] Instead, the regulation in the US concentrated on sectoral

[610] Microsoft has $540B of market capitalisation, Kleiner Perkins Caufield Byers 2017, p.324.

[611] Kirby 2008, pp.383–384.

[612] Although many states have enacted their own data privacy laws, eg California or Florida. Also, 'consumer privacy' is to some extent covered under s 5 of the Federal Trade Commission Act when the actions of firms are unfair or deceptive, see Hoofnagle 2016, p.145ff.

fields (like health services).[613] Apparently, the US authorities do not see serious problems justifying further regulation of their 'golden goose',[614] and, there is no sign that this approach will be changed in the near future. The proposal of the Consumer Privacy Bill of Rights evaluated under Barack Obama's administration in 2012 was eventually not put forward,[615] and Donald Trump in one of his first executive orders limited application of the Privacy Act to American citizens.[616] There is no inclination to privacy regulations in the US. In relation to regulation of technology "to do nothing is … effectively to decide that nothing should be done".[617] This suggests that in the globalised online environment the real chances to implement PMM need to be found outside the US.

So, in such an environment the real chances to implement PMM need to be found outside the regular state regulatory regime.[618] There are international political communities creating privacy regulations which differ between one another according to scope of their application, enforceability, and accountability.[619] Those privacy regimes overlap and interact in a complicated way and influence the national laws. The most influential of these regimes and their main regulations are:

- The European Union (EU),[620] with the Data Protection Directive (1995) and, recently, the General Data Protection Regulation (2016);
- OECD, with Guidelines on the protection of Personal Privacy and trans-border flows of Personal Data (1981, amended in 2013);
- The Council of Europe (CoE), with the important Convention for the protection of Individuals with regards to the Automatic Processing of Personal Data (so-called Convention 108 adopted in 1981).

---

[613] Eg Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[614] The Federal Trade Commission 2016, p.33.

[615] Initial proposal, The White House 2012; the Bill, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015.

[616] "Executive Order: Enhancing Public Safety in the Interior of the United States" 2017.

[617] Kirby 2008, p.383.

[618] That is to say, the relevant laws need to be aligned on a higher level, because of the weak position of the state in front of the above described processes (of globalisation).

[619] Bennett and Raab 2006, p.209.

[620] The EU is a sui generis entity. It has some elements of federation (eg legislation and a system of common courts).

The regulations of the European Union are first in this list because of their influence on other jurisdictions.[621] This is achieved mainly by the means of adequacy clauses in the EU Data Protection Directive (DPD) which allow transfers of personal data only to jurisdictions which have adequate level of personal data protection.[622] This motivates the countries willing to be recognised as 'adequate' to harmonise their law with the European one. The reason for this influence was explained by Bradford as a combination of market power of the EU, regulatory capacity, tendency to regulate consumer markets, and economic rationale which makes global companies adopt one set of global privacy rules which reflects the strictest standard – the European one.[623] This effect is also reinforced by direct applicability of the European law to foreign entities. The "aggressive geographic scope" of the DPD[624] is even wider in the new regulation, the GDPR.[625] Such unilateral regulatory globalisation has its limits,[626] but probably as long as Europe remains the significant market for global online service providers[627] the European data protection standards will be exported to other jurisdictions. This method addresses the problem of regulation of the services providers acting from abroad and will be described in detail in Chapter VII.

The instruments of the CoE and OECD served as important harmonisation mechanisms in the past,[628] but have not been actively developing privacy standards for a long time. Even though the OECD Guidelines were amended in 2013, this was rather removing limitations and adjusting the text to current standards than advancing new ones.[629] Therefore, it seems that the

---

[621] Bradford 2012; Greenleaf 2012.

[622] Greenleaf 2012, pp.77–78.

[623] Bradford 2012, pp.22–26; similarly, Goldsmith and Wu 2006, p.129.

[624] Goldsmith and Wu 2006, p.128. More details in Chapter VII.

[625] GDPR, Article 3.

[626] Eg sometimes global companies decide to implement some policies only for Europe, Fioretti 25 March 2016.

[627] Eg for Facebook Europe represents approximately 24 per cent of advertising revenue, Facebook ("2017 Q3 Results") 2017; for Google, the whole EMEA region brings 32.7 per cent of revenue, Google ("Alphabet - Q2 2017 Results") 2017, p.2.

[628] Details in Chapter VII.

[629] No new principles were introduced, mainly the accountability principle was developed to introduce privacy management programmes of data controllers (s 15), details in OECD Guidelines 2013, p.23 ff.

best place to implement PMM is the EU, as it exports higher privacy protection to other jurisdictions and this trend is likely to be continued. This is a pragmatic approach which aims to overcome the described problems by using institutions proven to be effective.[630]

Also, from the institutional point of view it is important that privacy regulations are overseen and enforced by competent and independent Data Protection Authorities (DPA). That is to say, the desirable privacy regime should have a DPA capable of supervising privacy management systems, so, having necessary powers to investigate powerful service providers. As will be shown in Chapter VII, most of the current privacy regimes in the selected jurisdictions have such DPAs. However, in the PMM model DPAs would not need to be as much involved in data processing operations as in the past (for example, with personal data licensing in Sweden and other European countries in 1970s[631] or with a system of registration of processing of the DPD).[632] Instead, PMM would re-introduce individuals into oversight of their own data which should be more effective with the support of third parties.[633] This increase of effectiveness should also be reflected in the regulatory operations of DPAs which would be needed only to supervise and resolve potential conflicts. So, DPAs could focus more on acting as standard setting bodies on the lower, non-statutory level, on being a competency centre, providing expertise and propagating those standards together with privacy education through the industry and the general public.[634] In light of increasing flows of personal data this should be a sensible shift.[635]

D Conclusions

Effective privacy management occurs when privacy regulation allows data subjects to exercise their informational autonomy and create a safe environment where data transactions can be performed in an easy and secure way. This can be achieved by the means of the Privacy

---

[630] But, if the US legislators want to regulate privacy and they find PMM a suitable model for it, that, of course, would be a desirable turn of action.

[631] Bygrave and Schartum 2009, p.157; Flaherty 1989, p. 95.

[632] See the DPD, Articles 18-21.

[633] See details in the next chapter.

[634] Bennett and Raab 2006 pp.133–143.

[635] Cf Bygrave and Schartum 2009, pp.160-162;

Management Model, which requires three sets of functions: controlling, planning, and organising. They form a prerequisite to indirect control over personal data exercised by data subjects (with the help from third parties) in the service providers' ICT systems by the means of technical and legal tools. Such a system could be applied to those providers of Internet services whose data activities breach informational autonomy. This could also enable regulators to deemphasise the overcomplicated consent procedure.

Such a regulation could be a win-win solution for all market participants. That is to say, it may be a non-paternalistic and more effective way of protecting groups and individuals who are vulnerable. Also, it should strengthen competition in the market and may correct many market failures associated with the current approach. Moreover, PMM may be seen as a tool which 'oils the wheels of commerce', because it eliminates important concerns related to consent, and creates an environment of trust between online service providers and data subjects.

PMM should be implemented with an adequate mix of regulatory 'tools' and by the actors which have the potential to do it successfully. To design such a system, the next chapter will analyse economic regulations to find a way to restore the balance of power in online services and to present a 'business model' in which PMM could be applied. This business model includes a set of measures to influence 'data markets' to improve informational self-determination and competitiveness, including the introduction of third parties, Personal Information Administrators. Chapter VI will then describe technology tools necessary for PMM and will check if they are feasible to implement. Finally, Chapter VII will describe the legal tools. According to what has been discussed above, those legal tools will be focused on data privacy laws and privacy rights and devised mainly for the regulatory regime of the European Union.

V Economic Regulation of 'Data Markets'

The previous chapter presented the Privacy Management Model (PMM), which is a tool to manage personal data in the ICT systems of online service providers by data subjects. It gives individuals the capacity to steer their own privacy processes by deciding what data about them are collected and how they are used. But, this model needs to be implemented in the context of actual online services in their 'data markets'. As explained in the previous chapter, this implementation should also help to correct market failure and overcome existing competition problems. This relates to achieving one of the goals of this thesis – the economics-related effectiveness. So, this chapter needs to bring these theories into a viable 'business model' in which PMM is applied to be a countermeasure to architectural and informational imbalances. As Chapter III explained how 'data markets' operate, now it is time to discuss what they lack to respect informational self-determination and to show how they can be influenced towards an effective privacy management.

This is presented in two steps. First, Part A shows the current state of market competition and discusses the ability of 'data markets' to provide data subjects with more effective privacy management themselves. In doing so, it identifies the particular reasons privacy is not a competitive factor. Also, it discusses self-regulation as an option to introduce privacy management. Second, Part B presents the set of market regulatory tools which aim to put service providers and data subjects on more equal positions. To that end, it presents a model in which Personal Information Administrators, a third party, are involved to help data subjects to understand and manage the privacy process. It also shows other measures for balancing their relationship with online service providers: introducing data portability, increasing their 'data sensitivity' by providing 'smart' transparency and expertise, and, last but not least, securing data subjects from uncontrolled tracking, in which their data 'leak' to undisclosed parties. All those measures form a 'business model' in which PMM is employed to balance markets and increase trust.

A Could 'Data Markets' Introduce Privacy Management by Themselves?

Market mechanism is often deemed to be an efficient way of distribution of goods which can regulate itself. Such 'hands off' approach is linked to neoliberal theories associated with the so-called Chicago school of economics.[636] But, as discussed in the previous chapters, this does not work well for privacy in 'data markets'. Now, it is the time to discuss why and to identify the characteristics of those markets responsible for problems. As 'data markets' support the creation of the largest global companies,[637] the first task is to verify whether they are competitive. This is because, as discussed in Chapter IV, introducing PMM should be aimed to increase competitiveness of the market.

1. *It is too early to find monopoly*

There are many signs that online business models (ie platforms) driven by network effects and economy of scale favour market concentration. Nevertheless, despite these problems there are also features of these markets which show their competitiveness and prevent the application of competition law. The discussion of all those factors also exposes problems which need to be overcome by choosing the appropriate methods for implementing PMM.

Some authors raise concerns whether and how competition problems are influencing privacy problems and if this should be addressed by competition law.[638] More specifically, data are often crucial for market performance, and in this respect may be seen as a source of market

[636] Acquisti, Taylor and Wagman 2016, p.450. This article offers an excellent review of economic theories and analyses of privacy; also, Ezrachi and Stucke 2016, p.22.

[637] See the previous chapter.

[638] Kuner and others 2014; Graef and Van Alsenoy 24 March 2016; European Data Protection Supervisor ("Report of workshop on Privacy, Consumers, Competition and Big Data") 2014.

power,[639] as a factor enabling collusion,[640] or as an element of harm theories.[641] So, they appear on many levels of the competition analysis. This is a significant issue, because if the 'digital markets' have tendencies towards monopoly, this would imply the need for the application of competition law or even creation of a sector-specific ex ante regulation as in other regulated industries (mainly infrastructural: railways, energy, or telecommunications). For example, monopolies are regulated to prevent harms arising from their actions. And, harms described in Chapter III could constitute a new type of consumer, privacy-related harm.[642] Such discussion in relation to Internet platforms is currently ongoing in many European countries.[643] The leading opinions towards regulation are from France (suggesting straightforwardly ex-ante regulation),[644] the European Parliament (suggesting 'unbundling' of Google,[645] and extending competition policy),[646] while Germany[647] suggests only small improvements to competition law, and the UK[648] seems to be reluctant to use any of those measures. Interestingly, in Australia, Canada, and New Zealand there seems to be no discussion about such regulation of Internet platforms at all.

There are arguments that the digital economy is tipping towards dominance of a few big players.[649] As shown in Chapter IV, the biggest Internet companies are also the biggest firms

---

[639] See Chapter III.

[640] Bundeskartellamt and Autorité de la concurrence 2016, pp.14–15. Competition Law varies between jurisdictions and, for example, tacit collusion (ie coordination of market actions between firms having collective dominant position) is not recognised in some jurisdictions, for example in New Zealand.

[641] Harm to consumers (eg price discrimination) or competition (eg exclusionary conduct), more in Bundeskartellamt and Autorité de la concurrence 2016, p.15 ff; see also a perspective on harms to competition in Graef 2016, pp.269–277.

[642] Eg European Data Protection Supervisor ("Privacy and competitiveness in the age of big data") 2014, p.26.

[643] House of Lords (HL Paper 129) 2016; Van Gorp and Batura (IP/A/ECON/2014-12) 2015; The Federal Trade Commission 2016; The German Monopolies Commission 2015; Conseil National du Numerique 2014; Chisholm and Jung 2015.

[644] Conseil National du Numerique 2014.

[645] Eg European Parliament resolution of 27 November 2014 on supporting consumer rights in the digital single market 2014/2973(RSP), s 15.

[646] Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.10.

[647] The German Monopolies Commission 2015, p.132.

[648] See conclusions in House of Lords (HL Paper 129) 2016, p.32.

[649] Eg conclusion in Interim Synthesis and OECD 2014, p.7.

in the world operating from the United States. Their market shares may indicate dominance in some markets.[650] For example, Google owns 92.31 per cent of the global[651] search market, 52 per cent of the web browser market (with Chrome) and 71.6 per cent of the mobile operating systems market (with Android).[652] Also, Facebook has 87.15 per cent of the global share of the social media market.[653] Furthermore, as this is mainly a two-sided market economy, the business side of the market can be assessed. Estimates show that Google and Facebook have together around 56 per cent of global digital advertising revenue[654] (53.6 per cent in NZ,[655] 53 per cent in the UK[656]). Other factors also indicate tipping towards dominance: network effects promoting market concentration,[657] economies of scale (advantages due to size or output),[658] economies of scope (in range of products),[659] high switching costs for consumers and businesses (ie disadvantages caused by switching provider),[660] high entry barriers, and limited opportunity for innovation.[661] However, the last three factors (switching costs, entry barriers, and innovation) are heavily debated.

Some authors are more convinced about the existence of such tipping than others. Ezrachi and Stucke describe the competition problems caused by a group of 'super-platforms' eliminating from their ecosystem those competitors, who challenge the business model based on personal

---

[650] However, it is only an indicative element as the definition of dominance differs across jurisdictions; see the discussion in OECD (OCDE/GD(96)131) 1996, pp.8–9.

[651] AU 94.08 per cent, CAN 90.59 per cent, NZ 95 per cent, UK 90.26 per cent.

[652] According to "StatCounter Global Stats" n.d. for March 2016-March 2017.

[653] AU 85.45 per cent, CAN 74.13 per cent, NZ 84.75 per cent, UK 79.62 per cent, "StatCounter Global Stats" n.d. for March 2016-March 2017.

[654] Desjardins 2016.

[655] Underhill 2016.

[656] Jackson 15 December 2016.

[657] Eg House of Lords (HL Paper 129) 2016, p.23; The Federal Trade Commission 2016, p.26; The German Monopolies Commission 2015, p.19; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.17.

[658] Eg The German Monopolies Commission 2015, p.21; Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.69.

[659] The German Monopolies Commission 2015, p.66; The Federal Trade Commission 2016, p.6.

[660] Eg House of Lords (HL Paper 129) 2016, pp.26–28; House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.4.

[661] House of Lords (HL Paper 129) 2016, pp.28–29.

data.[662] For example, Google removed the application Disconnect which eliminates advertisements from user devices from their application store (Play), because it "interferes with other applications".[663] Ezrachi and Stucke also claim that some companies have so much knowledge about the market that they de facto regulate them, which bears some resemblance to central planning in communist economies, but reinforced by computer algorithms,[664] and, that knowledge enables them to discern market trends and threats well before competition and government.[665] Other authors also find monopolisation,[666] and transferring the dominant positions to other markets.[667]

However, there are other opinions about dominance of Internet platforms. Some authors see more positive effects of platforms on competitiveness, namely increasing consumer choices, market transparency, and reducing search costs.[668] This is because undoubtedly consumers have access to more products and services by the means of Internet platforms. Additionally, many online markets, for example online travel portals, real estate, dating portals, shopping centres, or media, show signs of intense competition.[669] This may indicate that online platforms are not intrinsically tipping towards dominance, but may simply have tendencies towards this in some selected areas.[670] Furthermore, big Internet platforms usually occupy different markets (eg Google – search and mobile operating systems, Facebook – social networks, Amazon – online retail), and fiercely compete in other markets. Therefore, their strong position is seen as not secured.[671] There seems to be two main arguments for this. Firstly, risk of innovation and 'disruptive' market entry of a new player.[672] The evidence given

---

[662] 'Frenemies', Ezrachi and Stucke 2016, pp.145–202.

[663] Disconnect (Case COMP/40099) 2015, p.63; similarly, Cox 18 January 2017.

[664] They also ask an important question: should government compete to create its own algorithm and dataset? Ezrachi and Stucke 2016, p.212; also, The Federal Trade Commission 2016, p.60.

[665] Ezrachi and Stucke 2016, p.239; similarly, Prufer and Schottmüller 2017, p.2.

[666] Argenton and Prüfer 2012.

[667] Edelman 2015; Prufer and Schottmüller 2017, p.3.

[668] Eg The Federal Trade Commission 2016, p.3; extensive list in House of Lords (HL Paper 129) 2016, pp.9–12; World Economic Forum and Bain & Company 2011, p.5.

[669] The German Monopolies Commission 2015, p.20.

[670] House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.5.

[671] Haucap and Heimeshoff 2013, p.60.

[672] Eg House of Lords (HL Paper 129) 2016, p.32.

here is market dynamics and the fact that most of the big platforms are relatively new businesses. This suggests that the barriers to entry are low[673] and the incentives to innovation very strong.[674] Secondly, switching costs seem to be low on some markets due to so-called 'multi-homing' of customers, their ability to use different services in the same time.[675] For example, it is possible to use different search engines in parallel. These arguments make competition authorities very cautious in their declarations.[676]

Competition authorities are also not keen to see data-related privacy problems as relevant to competition law.[677] For example, in its decision regarding the Facebook/WhatsApp merger the European Commission clearly stated that "any privacy-related concerns flowing from increased concentration of data … do not fall within the scope of the EU competition law rules".[678] Nevertheless, privacy may be incidentally taken into account by competition law when breaching data privacy rules is used to restrict competition, as a competitive factor being a part of service quality, or potentially to assess an exploitative conduct.[679] So, competition authorities will be inspecting competition issues related to those Internet companies, because of their size and significance to the market,[680] but privacy is not their focus. This corresponds to the findings in the previous chapter, that their interest is limited to the problems of consumer and economic dimension of privacy.

So, given that it cannot be said that the 'digital markets' as a whole have some intrinsic problems, competition law may not be instrumental to implement PMM. The solution then seems more likely to lie elsewhere. To find it, it is necessary to verify why market forces do not support products on the market which offer more privacy over the others.

---

[673] House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.4.

[674] The German Monopolies Commission 2015, p.26.

[675] The Federal Trade Commission 2016, p.26; Evans and Schmalensee 2016, p.28.

[676] Conclusions of Bundeskartellamt and Autorité de la concurrence 2016, p.52 ff.

[677] See the second 'general observation' in Graef 2016, p.366.

[678] *Facebook/WhatsApp* (COMP/M7217) 2014, para.164; similarly, "the decision is without prejudice to the obligations imposed" by privacy law, *Google/DoubleClick* (COMP/M4731) 2008, para.368.

[679] Bundeskartellamt and Autorité de la concurrence 2016, pp.23–25.

[680] Eg. European Commission (press release IP/17/1784) 2017; European Commission (press release IP/16/1492) 2016.

2. *Why does the 'invisible hand' of the market not improve privacy?*

If data markets are not monopolistic, the 'invisible hand' of the market should be able to correct them to the optimal point where demand meets supply.[681] If privacy is important ('salient') for individuals (ie is an important factor considered in the choice of products), they should prefer service providers with more privacy-friendly offers over others.[682] In this way, providers would compete with concessions to their users and the 'invisible hand' of the market would steer all offers to an optimal point in which privacy concerns are balanced with attractiveness of the service providers' offers. In this approach, privacy is treated as a non-price element of the service, a part of the quality of the service.[683] As a result, unobservable market forces would lead to effective results.

The problem is that privacy seems to be not a significant parameter of competition and the above theory does not apply in practice.[684] This may be because individuals (assuming they know about collection of their data) lack awareness that they may use data to 'discipline' service providers, lack understanding of the value of their data, and, with regard to third parties, lack any contractual connection with them.[685] In respect of the value of personal data, it is well evidenced that customers are not 'data sensitive', ie they have problems with detecting privacy differences between service providers, due to the lack of information or problems with its assessment.[686]

These problems come from information asymmetry. This is because the differences in T&Cs are hardly observable for users, who mostly do not read them.[687] Furthermore, they do not see inferences made on the basis of their data. So, it is hard to weigh the unknown when they may only (imperfectly) assess that service providers have data of a particular kind. As a result, the only privacy-oriented competition which may take place is based on the overall perception of

[681] Trebilcock 1993, p.241; also, Smith 1776, p.187.

[682] Eg Nehf 2007, p.354.

[683] Stucke and Grunes 2016, p.119.

[684] Bundeskartellamt and Autorité de la concurrence 2016, p.25.

[685] House of Lords (OPL0055) 2015, p.20.

[686] Eg Acquisti and Grossklags 2005; Nehf 2007, pp.355–359; Acquisti, Taylor and Wagman 2016, pp.477–478.

[687] European Data Protection Supervisor ("Privacy and competitiveness in the age of big data") 2014, p.34.

a particular service provider as 'caring'. Such perception may be gained from statements about privacy on service providers' websites, but, this signal is often declaratory (eg 'your privacy matters to us')[688] and may be easily read incorrectly by customers. A general perception of service provider as being privacy-friendly may also be induced by providing individuals with some privacy settings in 'privacy dashboard' which, however, do not provide meaningful privacy management.[689]

So, if customers are not aware of privacy-related differences between service providers, they cannot make proper choices between better and worse ones. In this situation, platforms choose privacy strategies which maximise their profits and enable them to gain advantage over competition. As a result, in 'data markets' bad quality drives out a good one.[690] And, instead of reaching optimum, the market may be heading towards 'dysfunctional equilibrium' in which market participants that would like to compete with privacy may only sacrifice their profits.[691]

Another factor necessary to develop competition is the actual ability of users to switch between service providers. For some services, like social networks, switching costs are perceived as high due to network effects.[692] But, for others, for example for search providers, switching costs are more debatable because of 'multi-homing'.[693] It is possible to apply the lesson from telecommunications regulations, where switching costs were decreased by mandating interoperability of the services[694] and (much later) number portability.[695] Such interoperability may make sense only to those online services which exchange communications, eg social networks, but what actually could be applied to most online services is data portability,[696] the

[688] A great number of privacy policies actually start with "We care about your privacy" or include "Your privacy matters to us".

[689] See Chapter VI.

[690] Cf Akerlof 1970, pp.488–490.

[691] Farrell 2012, p.259.

[692] House of Lords ("Oral evidence from Daniel Zimmer and Thomas Weck") 2015, p.7.

[693] See summary of arguments, House of Lords (HL Paper 129) 2016, p.27.

[694] Zimmer, House of Lords ("Oral evidence from Daniel Zimmer and Thomas Weck") 2015, p.7.

[695] Directive 2002/22/EC (Universal Service Directive), Article 30; similarly, Telecommunications Act 2001 sch 1 pt 2 sub-pt 3.

[696] European Data Protection Supervisor ("Privacy and competitiveness in the age of big data") 2014, p.36.

ability of data subjects to move data to a new service provider. Moving data to a new phone or new computer is something well known and understood as necessary for consumers. Data portability is just an extension of this concept into the world of online services. Furthermore, it is already implemented in EU law[697] and, if successfully introduced, it would not only improve competition by decreasing switching costs and remedying user lock-in,[698] but also enable the market of re-using data for the benefits of data subjects[699] and keep it under their control. This will be further explored in Part B.

So, there is no sign of improving privacy by the invisible hand of the market in 'data markets' and privacy is not a barometer of service quality.[700] The main reason for this is lack of awareness of data activities. This suggests, as a minimum, a need to strengthen monitoring functions of privacy management, so the access to information about actual data and their use[701] and probably also a need for increasing competitiveness by data portability. Is there a chance for a self-regulation in this respect?

3. *Self-regulation is not a viable option*

The debate whether privacy should be improved using regulatory or self-regulatory tools has been taking place for at least 20 years.[702] It is probably enough to say that self-regulation is often understood as relying on current 'notice and consent' (or 'transparency and control') mechanism,[703] the failure of which has already been described. But, as there are signs that privacy protection may generate additional trust among consumers and self-regulation may be an opportunity rather than a threat,[704] the reasons for the reluctant approach of online service providers to develop a new privacy approach should be reconsidered. In this respect, Culnan

---

[697] GDPR, Article 20; more in Article 29 WP (WP 242 rev01) 2017.

[698] As it "goes to the heart of competition policy", Graef, Verschakelen and Valcke 2013, p.5 ff.

[699] European Data Protection Supervisor ("Privacy and competitiveness in the age of big data") 2014, p.15.

[700] See also House of Lords ("Oral evidence from Giovanni Buttarelli") 2015, p.5.

[701] To provide customers with information about advantages and disadvantages of the service, see the role of disclosure in Freiberg 2010, pp.167–168.

[702] It is well described in Acquisti, Taylor and Wagman 2016, pp.479–481.

[703] Acquisti, Taylor and Wagman 2016, p.479.

[704] Which was argued in Chapter IV; also, Bennett and Raab 2006, p.172; Culnan and Bies 2003, p.337.

and Bies gave two such reasons in 2003: risk created by voluntary commitment, and lack of a guarantee that benefits will outweigh costs.[705] 14 years later, in the age of Big Data, to those two reasons which are still valid should be added additional one, that data are an asset which gives a competitive advantage.[706] The only firms that test using statements about privacy to distinguish themselves from competitors are those whose business model is less dependent on personal data, such as Apple.[707] For all others, the online business models not only favour 'sharing', but put data in the centre of business activities. So, those companies believe that their business model prevails over regulations targeted to preserve privacy.[708] Also, there is a long history of failed self-regulation initiatives,[709] some of which will be also presented later in this thesis.[710] What needs to happen to convince service providers to introduce self-regulation?

According to Bennet and Raab, there are several groups of conditions for effective self-regulation to evolve related to: international pressure, the structure of industry, technological changes, and the amount of publicity.[711] The most promising (to support PMM) seems to be international pressure, because it has proven to be effective. That is to say, the American ICT companies were pressured towards self-regulation after the enactment of the Privacy Directive by the EU in 1995. In that case, the threat of cutting off the American industry from accessing the EU's large market provided the EU with bargaining power to demand better protection of personal data of the Europeans.[712] As self-regulation was an alternative to regulation, the industry developed a plethora of self-regulatory schemes called "the Directive's bastard offshoots".[713] This all led to the development in 2000 under the auspices of the US Department

[705] Culnan and Bies 2003, p.336; also, conclusions about why companies do not invest in technologies of privacy protection in London Economics 2010, p.x.

[706] See Chapter III.

[707] Apple's business model relies more on selling terminals, so they can use this argument, Greenberg 6 August 2015; Hernandez 17 March 2015.

[708] See the comment of Giovanni Buttarelli about meeting the Silicon Valley companies in 2015 in House of Lords ("Oral evidence from Giovanni Buttarelli") 2015, p.5.

[709] Gellman and Dixon 2016.

[710] Eg 'Platform for Privacy Preferences' and 'Do Not Track' in Chapter VI.

[711] Bennett and Raab 2006, pp.172–174.

[712] Shaffer 1999, p.424.

[713] No because they were illegitimate, but because they had been not planned; see more in Shaffer 1999, p.433.

of Commerce of a self-regulatory scheme called 'Safe Harbour'. That scheme, containing a voluntary self-certification mechanism for companies wishing to be recognised as providing adequate level of protection was not perfect,[714] but survived 15 years despite numerous critical reviews,[715] until it was finally invalidated by the European Court of Justice in *Schrems*.[716] It is quite paradoxical, that globalisation brings the threat of exporting data to the jurisdiction where standards are lower, but also the opportunity to use higher privacy standards to leverage standards in other countries.[717] The case of Safe Harbour has also shown that 'data industry' is well organised, and capable of delivering self-regulation.

Other sets of factors increasing motivation to self-regulate related to technology and the level of publicity seem to be less effective.[718] New technologies, which introduce heavy data use may increase the perception of risk for the companies. But, as it could be seen on the example of the introduction of Big Data, new technologies are rather used to showing that current legal rules are too stringent.[719] Similarly, the impact following incidents of privacy violation is relatively low and short-lived.[720]

So, self-regulation of the industry seems very unlikely, unless it is introduced when the threat of regulation is imminent. Such a threat is likely to be effective if it comes from a significant market outside the US. The general conclusion from this Part is that 'data markets' cannot be relied on to implement more efficient privacy management by themselves. So, the next question is how to influence or modify them to implement privacy management.

---

[714] The list of deficiencies can be found in Dhont and others 2004, p.105 ff.

[715] Dhont and others 2004; Connolly 2008; Connolly and Dijk 2016; Bendrath 2007, pp.10–13.

[716] '[A]s compromising the essence of the fundamental right to respect for private life ...' Case C‑362/14 *Schrems* [2015], CJEU, para.93.

[717] Shaffer 1999, p.437.

[718] Bennett and Raab 2006, pp.172–173.

[719] Eg opinions from industry in Cate and Mayer-Schönberger 2013.

[720] Acquisti, Friedman and Telang 2006, p.12; however, some breaches could be in this respect different when handled improperly, Wiener-Bronner 2017.

B How to Influence 'Data Markets' to Improve Informational Self-determination

Knowing the nature of problems of competition in 'data markets', it is time now to describe a set of solutions. These solutions aim to balance the asymmetry of market power between data subjects and service providers by implementing PMM, 'nudge' the market towards recognising privacy as a competitive factor, and increase competition by decreasing switching costs and lowering barriers to entry. The inspiration for them comes from Porter's analysis of competitive forces – the so-called 'Porter's five forces'.[721] Applying this analysis, increasing power of data subjects as suppliers or customers[722] can be done, for example, by concentrating (grouping) them, introducing some intermediate customers, limiting the availability of their data from third parties, increasing their capacity to change service providers (by decreasing switching costs, standardising the services), or increasing sensitivity about prices (here, price in data, so 'data sensitivity').[723]

The first section of this Part shows how to leverage the power of data subjects through introducing third parties, Personal Information Administrators (PIAs), which could act as intermediate customers grouping data subjects and supporting them in privacy management. They are a crucial component of the PMM implementation, because they provide data subjects with necessary architectural tools[724] and expertise. Then, the second section examines how to increase market competitiveness by introducing data portability. This could reduce switching costs and enable a completely new market for services for data subjects based on their data.

The third section considers how to increase the 'data sensitivity' of individuals, which was one of the main market problems indicated in the previous Part. It is argued there, that this could be achieved through a combination of 'smart' transparency regulations providing the right amount of information to subjects and advice from PIAs. Finally, the fourth section

---

[721] Porter's Five Forces is a succinct but powerful description of competitive forces influencing competition in any given industry. It may be used as a starting point to analyse strategic position of a company. And, it is possible to look on the personal data market as on the specific industry where data are the product. The original, Porter 1979; newer version, Porter 2008.

[722] In the two-sided markets data subjects are suppliers of their data, and, in the same time, customers of retail services.

[723] Based on a general analysis of the power of suppliers and buyers in Porter 2008, pp.82–84.

[724] Details in the next chapter.

suggests ways of securing data subjects from unwanted tracking, which is aimed to secure and get individuals' data supply under control and guarantee their position as the only source of their own data (or, in other words, secure the leak of their 'data money'). In this way, this Part presents fully the 'business model' showing how to apply PMM in the market.

1. *Employing Personal Information Administrators*

Third parties acting as intermediate customers could play a significant role in data markets. They could be helpful in achieving both of the goals of this thesis: to achieve better privacy management by individuals, and to make data markets more competitive and more effective. They may support individuals in exercising their autonomy and provide them with necessary skills and expertise to achieve the former goal. Also, they may help to achieve the latter goal by helping the competition by aggregating power of data subjects and providing more transparency across different service providers. However, they should not be able to benefit directly from data. Moreover, they even should not hold all personal data of data subjects by themselves or be positioned in a data flow, because this would give them incentives to benefit from these data.[725] Instead, their incentives should be to help data subjects in privacy management, and revenue from using personal data would create a conflict of interest. Also, allowing them to hold all personal data would create an even more powerful actor on data markets than service providers.

The preferred business model of implementing PMM is to allow these intermediaries to act on behalf of data subjects to manage personal data in the systems of service providers.[726] They would administer personal information on behalf of individuals, hence the name Personal Information Administrators (PIAs). In this scenario, PIAs are not in the flow of all personal data, but in the flow of those personal data related to privacy management (management

[725] Footnote 77 in Betkier ("Individual Privacy Management") 2016, p.334.

[726] Ibid., p.326.

data).[727] They include all data necessary to exercise privacy management functions. Such a scenario is shown in Figure 16.[728]

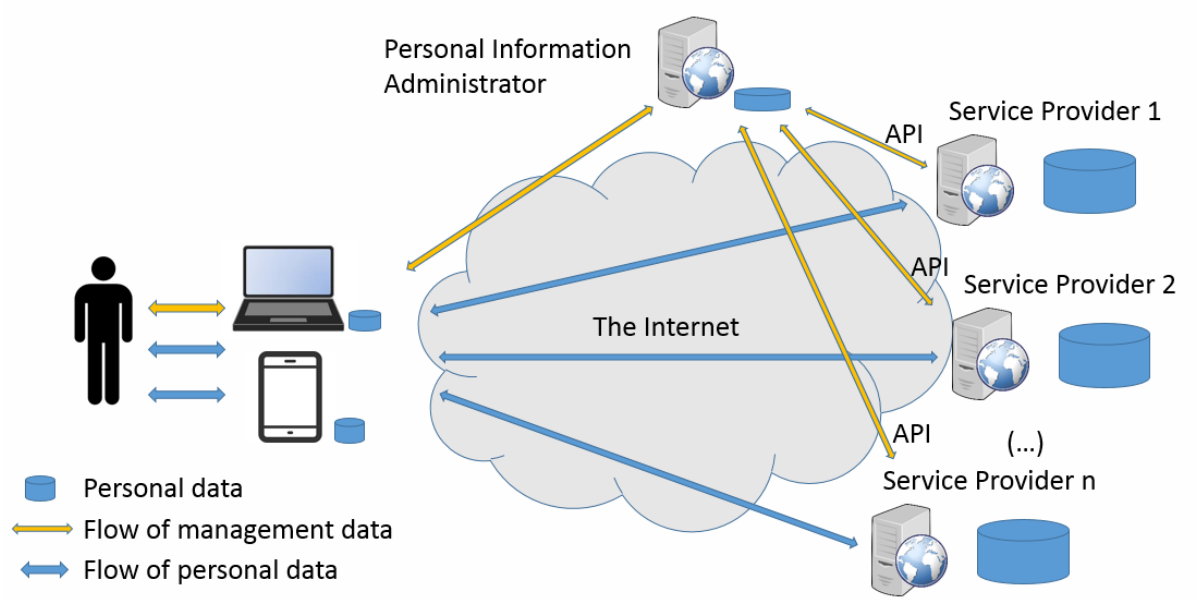


Figure 16 Personal Information Administrator acting for data subjects to enable and facilitate the flow of management data

This presupposes the creation of flow of management data, which includes the protocol of exchange of such data from data subject to PIA and from PIA to service provider, and an interface to remotely (and securely) manage personal data in the ICT systems of Service Providers.[729] This interface, Application Programming Interface (API) enables PIAs to build a software tool which integrates the management of data in the ICT systems of multiple service providers. In this tool, the privacy preferences of data subjects (comprising their privacy policies) are transformed into controlling decisions over data. In this way, data subjects have a one-stop shopping interface from which they could manage their privacy, see what is being collected and how it is used.

Also, data subjects should receive from PIAs some unique identifier of their 'account' (or other form of reference to) which they could use to point service providers to their privacy

[727] This idea was inspired by the concept of Next Generation Networks which separates functions (and transfers of data) related to control and management of services from other functions (and data transfers), International Telecommunication Union (ITU-T Y2011) 2004, p.5 ff. Such decoupling enables the network to provide its users with broader range of more scalable and interoperable services.

[728] Betkier ("Reclaiming personal data") 2016, p.11.

[729] Technologies necessary to build this are explained in the next chapter.

policy kept there. This identifier could be used when initiating each new service relationship[730] which requires personal data use (eg new mobile or desktop app, Internet browser settings, new Internet-enabled sensor, personal assistant). Such an exchange could look like the one shown in Figure 17 below.[731]

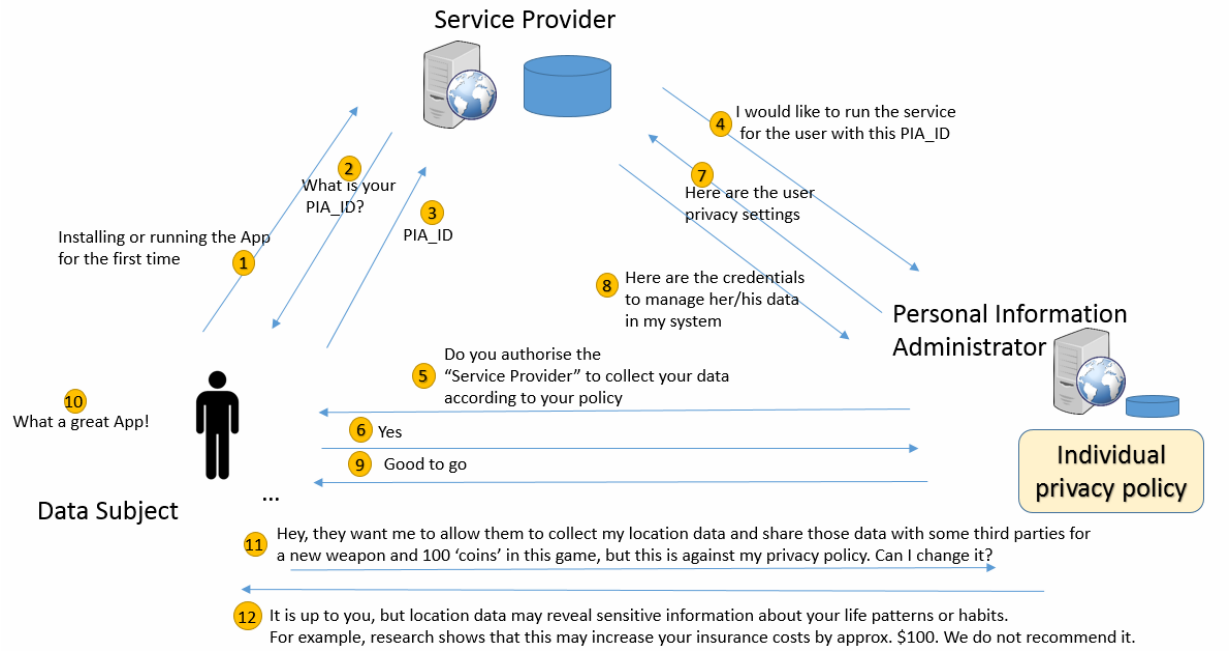


Figure 17 Example of the exchange of communications with PIA during the initiation of a service and afterwards

In the example from Figure 17, PIA is involved in the initiation phase of the relationship to communicate and enforce the data subject's privacy policy. It also shows how in the later stages of the relationship PIA may provide expertise about data collection and use.

The main advantage of this scenario is that it does not presuppose either changing current business models of the service providers on the market, or changing data flows. The data stay where they are and may be used as they are currently being used, provided that individuals have control over that use. In such a scenario, the PIA is not engaged in economic transactions with personal data, so they are not interested in increasing the amount of data processing. Those PIAs may be state agencies, privacy advocates, or firms whose business models are

[730] This bears some resemblance to a personal bank account number, but, the number is used to contact the PIA, download and apply the individual's privacy policy and initiate data management in relation between PIA and service provider.

[731] Cf ideas in conclusions of Neisse and others 2016, p.43 ff. This message exchange is exemplary, it is not based on any particular technical protocol, but User-Managed Access (UMA) protocol has some similar functionalities.

based on privacy management. This depends on the model applied in a given country and choice of data subjects. In a liberal model, PIAs may compete with their services providing users with additional functionalities. However, they should receive no revenue from service providers nor their own revenue from personal data,[732] because that creates a conflict of interest. So, in a model which does not rely on subsidies from public or private sources they need to operate a service based on payments from individuals, probably in the form of subscriptions.[733] In a digital economy the success of such business model depends really on the scale of their operation, as small payments from many users may be enough to cover the costs of setup and maintenance of PIA.[734] In any model, the nature of the relationship between the PIAs and data subjects should be similar to the relationship between professionals (lawyers, doctors, finance advisors) and their clients. Trust in such intermediaries is easier to establish than trust in all possible service providers.[735]

The idea of PIA as an external third party is inspired by two concepts discussed in the literature: Identity Management (IM) and Personal Information Management Systems (PIMS), albeit differing significantly from both of them. IM systems aim to confirm and securely use the identities of individuals. So, they protect privacy in the part in which they protect personal data used as the attributes of identity.[736] There was also a long-standing idea to wrap privacy protection around IM, which probably started with the concept of 'identity protector', ie a system hiding the identity of the data subjects behind their pseudonyms.[737] But, most of the current Internet services, especially the bigger ones, operate in a model in which they identify users based on their own sets of personal data, so the use of external IM is redundant for them.[738] Also, data subjects would still need to provide their personal data to service providers

[732] Also, they should not store personal data other than management data. Having said that, storing by PIAs some personal data related to data subjects' accounts and transactions is inevitable.

[733] The possible extent of their services is shown in Chapter VI describing technology they would use, and in Chapter VII describing the relevant laws.

[734] At this point the existence of start-ups in this area (eg 'BitsaboutMe', 'Datum') shows the potential, but the real test is achieving a scale, eg 10,000 – 100,000 users willing to pay $5-10 monthly for such a service.

[735] Frankel 2001, p.466.

[736] In computer science the distinction is sometimes put on unlinkability between the data and a person, eg Pfitzmann and Hansen 2010, p.34; Fritsch (D21) 2007, p.10.

[737] Van Rossum 1995.

[738] Danezis and Gürses 2010, p.10.

to use their services.[739] So, although the IM as a third party could bring some benefits to individuals (eg single sign-on), those benefits do not address privacy problems because IM does not give control over data. So, even compulsory introduction of an IM provider into the service flow (eg by regulation) would not introduce privacy management. Also, from the perspective of a service provider this would mean in some business models losing a gatekeeper position and completely reshaping their business model,[740] which is difficult to introduce.

Personal Information Management Systems (PIMS) provide some ideas in the concept of PIA. The name PIMS covers a few new concepts "increasing individuals' control/ownership and privacy of their data"[741] such as Vendor Relationship Management (VRM), Personal Data Stores (PDS), and 'MyData'.[742] These are all ideas for leveraging customers' positions by putting them in the central position of the environment and deciding about their data. This seemingly started with 'Doc' Searls coining the term Vendor Relationship Management (VRM). VRM is a way to organise relations between customers and different vendors to guarantee independence from them by making them fully empowered actors in the marketplace.[743] This is supposed to change the economy from an 'attention economy' in which companies try to guess what consumers want, to 'intention economy' in which consumers share their intentions with the business.[744] The website of 'Project VRM' enumerates principles, goals and characteristics of tools to be made.[745] This seems to boil down to some narrower sense in which individuals are provided with collection centres of their own personal data, which they could then selectively share, retaining control over them.[746]

---

[739] OECD (DSTI/ICCP/REG(2008)10) 2009, p.17; see also Jacobs 2010, pp.297–298.

[740] This could be even detrimental for data subjects as an IM provider in a gatekeeper position could monopolise the market. See the unsuccessful case of Microsoft Passport, Danezis and Gürses 2010, p.7; such an idea was also used in a novel, Eggers 2014, to show a path to domination of one service provider.

[741] 'Berlin Memorandum' n.d.

[742] Also, 'personal data spaces' or 'personal data vaults', European Data Protection Supervisor 2016, p.5.

[743] Analogical to Customer Relationship Management (CRM) used by business, "Project VRM" n.d.

[744] Searls 2012.

[745] Hosted by Berkman Center for Internet and Society at Harvard University "Project VRM" n.d.

[746] VRM goals in "Project VRM" n.d.

So, although the main idea of VRM, customer independence, is in line with PMM,[747] it seems to apply the controlling model of PDS, which relies on collecting and guarding all personal data in one place.[748] That is to say, data are expected to be on the customer premises (or on the premises of VRM system provider) "stored in … personal, secure 'digital safe deposit boxes'".[749] This model presupposes that the PDS provider is put in the data flow and collects all the personal data, as in Figure 18 below. Then, it acts as a 'firewall' which enables the flow to service providers of only an agreed part of data.

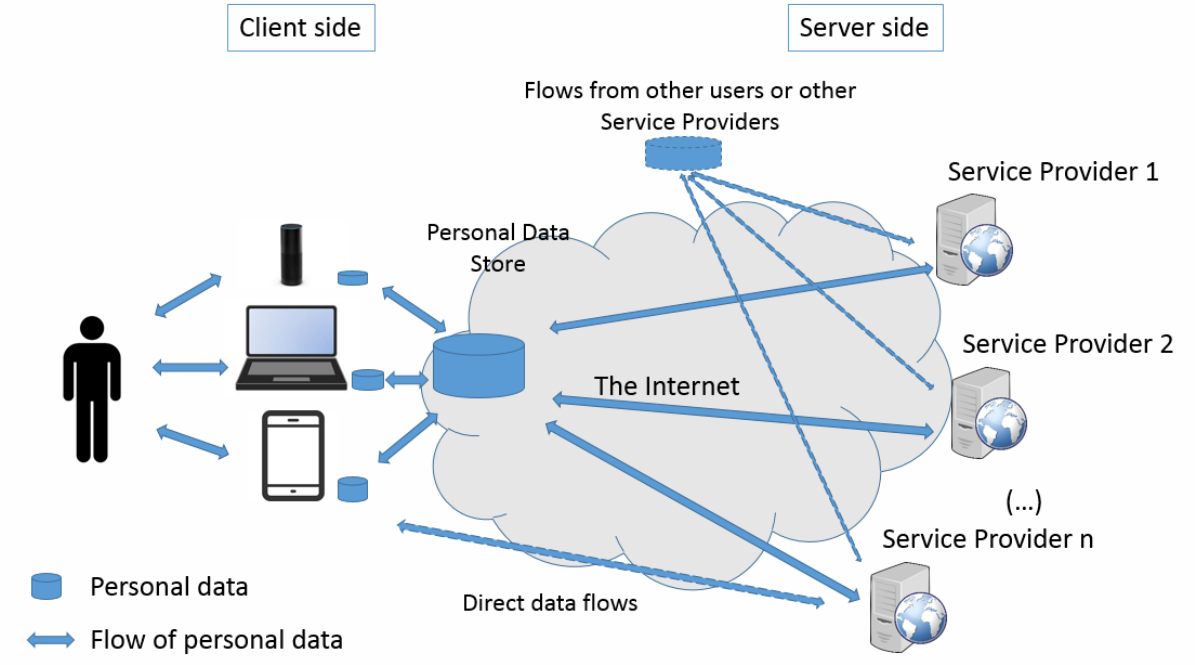


Figure 18 Personal Data Store model

PDS may be provided either as a local storage of data, or as a cloud-based, virtual server.[750] The product ideas include Virtual Individual Servers[751] or Databoxes,[752] which could securely hold the whole range of personal data such as communications, financial, location, or social network data.[753] However, as shown in Figure 18, the idea to put all personal data in one place may be unrealistic. Firstly, there are direct data flows resulting from tracking activities

[747] However, it seems to recognise only the economic value of privacy.

[748] Brochot and others 2015, p.2. PDS are also called personal data vaults, lockers, or personal clouds.

[749] See advantages of VRM by Graham Sadd in P2P Foundation 28 January 2012.

[750] Brochot and others 2015, p.20; de Montjoye and others 2014, p.2.

[751] Cáceres and others 2009.

[752] Chaudhry and others 2015.

[753] Eg "BitsaboutMe" n.d.

indicated in the picture by the dashed arrow at the bottom.[754] Secondly, other dashed arrows show that individuals (as recognised in Chapter III) are not the only source of their own personal data. Their data are acquired from data brokers, other service providers, or even other individuals (eg 'tagging' others in photos). So, to build a PDS it would be necessary to redirect all flows of personal data to PDS and make PDS the only source of personal data. Such 'sealing off' of personal data does not seem to be feasible. Furthermore, even if it were possible, it would require service providers to rely only on data from PDS. This means resignation from their actual business model (based on collecting personal data and processing them on their own) and disabling many services which require the location of personal data on their premises (eg Big Data). All this leads to the conclusion that collecting all user data in one place cannot be implemented in the current online environment.

Another problem of VRM is that it does not foresee giving additional capacity to plan, organise, and control to customers. So, it assumes that they could express their demand for services on the 'open market' stating their own terms of those services which vendors could negotiate.[755] There is little chance for successful implementation of such functionality because of the current imbalance of power and also because of the importance of adhesive contracts.[756] Nobody negotiates T&Cs with Internet service providers, and the same follows with banks, energy providers, or telecommunication services. Many elements of those contracts cannot be negotiable by their nature. This does not mean, however, that online services cannot be adjustable to some degree to individuals' requirements. But, VRM seems to not emphasise the need for common standard for categorisation of data and data uses necessary for such adjustments. Also, control in the VRM concept is centred on data subjects' own 'digital deposit boxes',[757] and does not extends to the ICT systems of service providers. For example, VRM seems to foresee that individuals can extend control over data by concluding additional agreements to delete unnecessary data afterwards,[758] but there is no solution for monitoring data collection and uses.[759] Finally, all these ideas do not show a viable path between the

[754] Tracking by service providers, not only by third parties.

[755] "Project VRM" n.d.

[756] Cf also points 1 and 2 of the VRM critique in Hill 23 January 2009.

[757] Principle 2 and goal 2, "Project VRM" n.d.

[758] Goal 4, "Project VRM" n.d.

[759] Cf enforcement problems, European Data Protection Supervisor 2016, p.10.

current market and the desired model,[760] which may be the most crucial part of transition to a user-centred economy. But, to the effect that VRM is just a high-level vision, it can be said that PMM and PIAs share its philosophy.[761]

Another, PIMS-like idea for empowering customers was developed by the Finnish programme called 'MyData'.[762] Instead of concentrating on individuals as customers in particular sectors, it concentrated on creating common, human-centred infrastructure for many sectors which could ensure data interoperability and portability.[763] The idea is that individuals, through a trusted third party called here 'MyData Operator', could exercise 'consent management' authorising the use of their personal data by different service providers.[764] This idea is similar to PMM, as it does not presuppose central location of data. However, 'MyData' seems to be focused on consent, probably because of the requirements of EU regulations. Although this consent is understood as dynamic, easy to comprehend, machine-readable, standardised and managed in a coordinated way,[765] this cannot provide privacy management because of its inherent problems (as discussed previously). So, many problems of 'MyData' are similar to those of VRM. That is to say, it does not offer any data management model and any idea how to reach its vision starting from the online services as they are now. Therefore, PMM could be an interesting complementary tool to 'MyData'. The Finnish project produced some technical documentation,[766] and had a first implementation in a 'sandbox' academic environment.[767] Some of the technical tools used there, such as Kantara Initiative's consent receipt specification,[768] will be discussed in the next chapter. 'MyData', like some other concepts of PIMS, seems to put more emphasis on the concept of data portability, which will also be discussed in the next section.

---

[760] Similarly, European Data Protection Supervisor 2016, pp.13–14.

[761] As many other tools, concepts, standards, or organisations very loosely related to each other listed at "VRM Development Work - Project VRM" n.d.

[762] "MyData" n.d.

[763] Poikola, Kuikkaniemi and Kuittinen 2014, p.4.

[764] Ibid., p.5.

[765] Ibid., p.7.

[766] Alén-Savikko and others n.d.

[767] Su and others 2016; Honko 2016, p.10.

[768] Version 1.0.0, April 2017, Lizar and Turner 2017. See the next chapter.

In conclusion, the third party Personal Information Administrators should be put in the flow of management information, the information related to management of personal data. They should provide data subjects with a software tool which integrates the management of data in the ICT systems of a number of service providers via their Application Programming Interfaces. In such way data subjects would have a one-stop shopping tool to manage their privacy. Also, PIA should be conveniently integrated into initiation of any personal-data related relationship with a new service-provider, and should provide expertise in the case of renegotiating the terms of such contracts. The main advantage of this scenario is that it neither presupposes changing current business models of the service providers on the market, nor changing data flows, so it enables a relatively smooth transition from current online services to a human-centred model.

2. *Increasing competition by data portability*

As indicated previously,[769] data portability could help competition by increasing users' ability to switch between service providers.[770] In this respect, it would resolve those reasons for users' lock-in related to their data. This should have the effect of decreasing the competitive advantage of service providers arising from possession of vast amounts of data.[771] It could also help reduce barriers of entry, because new service providers could benefit from their customers' existing data. This idea is incorporated in PMM to the extent to which data are under the control of individuals and could be at any time requested (or downloaded) by them. Importantly, those data should be in a format which enables the data subject to easily reuse them.

This idea seems to be one of the most important for 'MyData'[772] and some other PIMS.[773] Some of those ideas produced practical results important to this thesis. The first such project was not very successful. The UK Government announced an initiative called 'mydata' in 2011

[769] In Chapter IV and in Part A above.

[770] Van Gorp and Batura (IP/A/ECON/2014-12) 2015, p.9.

[771] Defined by uniqueness of those data, House of Lords ("Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung") 2015, p.16.

[772] Poikola, Kuikkaniemi and Kuittinen 2014, p.3.

[773] Also, Gurevich, Hudis and Wing 2014, p.6 ff.

(renamed later to 'midata'), which was about empowering individuals by enabling them to access and use data held about them by businesses.[774] Shortly afterwards this was limited to regulations in a few sectors,[775] from which only banking actually delivered the functionality to import some transaction data from bank accounts and transmit them to a company comparing banking offers.[776] The second project, the French MesInfos lead by Fondation Internet Nouvelle Generation, developed an idea called SelfData.[777] The idea was to put "the collection, use and sharing of personal data by and for individuals, under their complete control" and design it "to fulfil their own needs and aspirations."[778] This relied on concentrating data[779] in PDS,[780] and was very similar to the idea of VRM described above. However, this project also had a pilot study, which gave a great deal of practical insight into what is necessary for individuals to gain access to their data. Researchers found that the individuals participating in the study had greater awareness of data use and, since they had more control over data (in their PDS), they also more easily engaged in exchange of their data with firms. By 'sharing back' the data to the individuals the commercial advantage moves back towards them and, furthermore, a completely new market opens for reusing those data in the interest of individuals.[781] However, implementing such a solution is neither easy nor quick. There is a need for protocols and data formats allowing exchange of data. Such work has already started in the health sector,[782] and needs to be followed by other sectors.[783]

So, to sum up, data portability is an important concept which could increase competition in the market and put individuals in the position of decision makers about their data. But, to make

---

[774] Cabinet Office (URN 11/749) 2011, pp.16–20; Shadbolt 2013.

[775] That is: energy supply, mobile phone sector, current accounts, and credit cards. Cabinet Office (URN 12/1283), p.5.

[776] Some information can be found at pcamidata.co.uk n.d.; HM Treasury 26 March 2015; Jones 28 March 2015; Freeborn 8 April 2015; the example of comparison services, Bater n.d.

[777] Fondation Internet Nouvelle Generation ("MesInfos project").

[778] Fondation Internet Nouvelle Generation 2015, p.1.

[779] Types of those data are described in Albarède and others 2013, p.3.

[780] See the concept diagram in Fondation Internet Nouvelle Generation 2013, p.2; also, Abiteboul, André and Kaplan 2015.

[781] Fondation Internet Nouvelle Generation 2015, pp.3–4.

[782] 'Open mHealth' n.d.; Estrin April 2013.

[783] Those standards may evolve also from Universal Business Language standard, OASIS n.d.

an informed decision, data subjects should be able to distinguish the levels of privacy protection offered by service providers.

3. *Increasing 'data sensitivity' by monitoring and advice*

As discussed above, data portability should be accompanied by increasing 'data sensitivity'[784] of data subjects, ie their understanding of the value and importance of their data. As the current approach of providing information through T&Cs or privacy notices does not work,[785] there needs to be a smarter, more user-centric way to inform users. To enable market forces to operate and build trust[786] privacy needs to be a verifiable, accountable factor. To that end, individuals should be able to understand what they are disclosing to service providers and how this affects them, therefore how those data are used and the possible consequences of such use.[787] This could be briefly explained in the context of particular data using the framework of possible privacy problems: values-related (what harm can be inflicted and how this may occur), and economic (what is the possible economic consequence of particular data use).

Transparency (or monitoring) as a part of the controlling function of PMM aims to show data subjects their privacy processes with all data, data uses, and actors involved.[788] It means that privacy practices need to be visible and understandable for data subjects. As 'sunlight is the best disinfectant',[789] service providers, knowing that they are seen by their customers and regulators, may be forced to deliver better services.[790] It seems that data subjects could be effective in monitoring many categories of problems related to their own data. This is because they know best their own privacy preferences, see the improper use of their data, and feel negative impacts of privacy invasions. But, such transparency should strike the right balance

[784] Per analogiam to 'price sensitivity'. This could achieve the same effect as making quality problems visible, Yeung 2005, p.367.

[785] Also, Telefonica and Centre for Information Policy Leadership 2016, p.8.

[786] Or, in other words, to remedy market failure, avoid distrust and deadweight losses (see previous chapter).

[787] Cf price sensitivity in Porter 2008, p.84.

[788] Cf regulatory tools of 'information provision', Freiberg 2010, p.120; also, 'communication' instruments, Morgan and Yeung 2007, p.96.

[789] Attributed to J Brandeis.

[790] Also, Diaz, Tene and Gürses 2013, p.950.

between the amount of information and their meaningfulness,[791] which is difficult to achieve because of complexities of data and data uses. In this respect, many companies use architectural tools such as 'privacy dashboards', portals, apps to provide users with information and choice.[792] There are also technical protocols to express privacy policies and preferences.[793] All these technical tools seem to work much better than 'traditional' disclosure through T&Cs. These practices will be analysed in the next chapter, to find the best ideas for organising and presenting types of data and data uses in a way which would be clear and efficient for both parties. It seems that some standardisation in this respect is inevitable, and the regulation should eliminate confusion what particular data types mean in a given service.

But, transparency is not enough and it needs to be complemented with knowledge about data provided within the context of data requests from service providers.[794] This is because data subjects are often not rational decision makers capable of evaluating information and acting upon it. This cannot be fixed only with education about data uses; it needs to be effective advice from an independent expert provided at the right moment.[795] PIAs should be able to provide this part of the 'data sensitivity' functionality – explaining to users how the use of their data may affect them in non-economic and economic ways and what their options are. That should not be based on fear, but on providing relevant knowledge-based examples which show the real costs of particular data requests. This is because, as illustrated in Figure 17 above showing the example of the exchange of communications between the parties, those requests are often declared in the language of particular services. The benefit the data subject has from using the service also needs to be compared to the costs of data disclosure. Furthermore, it may be possible to adapt this to the particular type of customer with particular language and capabilities to understand (eg youth, elderly).

In such way it would be possible to address not only individuals' deficit of information, but also the deficit of necessary skills and expertise to enable them to make a meaningful choice. Disclosure would also be limited only to situations which enable choice, which could avoid

[791] Ben-Shahar and Schneider 2011, p.721.

[792] Cf Telefonica and Centre for Information Policy Leadership 2016, p.6.

[793] Eg W3C (P3P) 2007.

[794] Cf Telefonica and Centre for Information Policy Leadership 2016, p.11.

[795] Cf ibid., p.15.

problems of disclosure regulation which tend to bombard people with useless (and costly) disclosures in situations which do not enable any choice. As a result, individuals could understand the service providers' offers aiming to collect some of their personal data and respond to it.

But, as public scrutiny is not always the best 'disinfectant' in the case of privacy, because publicising furthers dissemination of private information,[796] privacy management should be accompanied by capacity to make effective complaints against service providers. If the potential consequences of complaints initiated by users are also under the scrutiny of regulators or courts and result in a material impact on service providers, the whole mechanism would work much better. This is especially important when the choice of service providers is limited.

4. *Securing data subjects from uncontrolled tracking*

The last element of the PMM 'business model' is related to securing individuals from uncontrolled 'leaks' of their data. This is important, because data subjects currently do not know when they are 'paying' for the services with their data, how much, and to whom.[797] In economic terms, this puts them in a losing position in a bargain, because they cannot control supply of their data. This also infringes the dignity of data subjects, because others have access to information about them without their knowledge or control.

Tracking consists of two separate problems: the problem of tracking by service providers and the problem of tracking by third parties.[798] Tracking by service providers could be managed by using PMM. But, in the current state of affairs, personal data are also collected by third parties which are sometimes not known to data subjects. Such tracking can be performed on different technical levels of a terminal device (eg computer or mobile phone): in web applications (ie visiting websites), applications (eg mobile 'apps'),[799] operating system (eg

[796] Similarly to 'Streisand effect', where attempting to suppress information attracts more unwanted attention.

[797] See Chapter III.

[798] Ie those who are not a party to the online contract.

[799] See overview of these categories, Neisse and others 2016.

Android),[800] or by monitoring from outside (eg sensors of Internet-enabled devices like TV).[801] As explained in Chapter III, this is performed by parties who use their relationships with service providers to collect personal data from data subjects and use those data for their own goals.

Such a problem of 'leaking' personal data to undisclosed third parties should be addressed also on a non-technical level. Firstly, responsibility for such tracking should be fully attributed to service providers.[802] This is because they are providing the computer code (program) uploaded and executed on customers' devices,[803] for example, as a web application or as a mobile app. So, they have to put there that part of the code which refers to the third parties, the execution of which results in sending those third parties personal data of data subjects. If they are in charge, they should take responsibility for collecting data. That is to say, they should change their business so that it would not be reliant on the third parties undisclosed to data subjects. But, there are also some important exceptions related to necessary activities performed by third parties. For example, some third parties may collect data for the sole purpose of transmitting data over the network.[804] Secondly, the relevant regulation should also include providers of software (such as web browser) which may be made responsible for providing software which enables securing data subjects from third party tracking.[805] In this way they could be secured by both service providers and providers of their software, which could be the same company (eg Google provides web browser Chrome and mobile operating system Android). It is also possible to link privacy settings of the browser with an individual privacy policy held by PIAs, which would not only be convenient but would also provide data subjects with consistent protection.

---

[800] Also, Achara 2016, p.7 ff.

[801] Eg Angwin 9 November 2015; Hern 9 February 2015; Gibbs 13 March 2015.

[802] Spiekermann and Novotny 2015, p.184; The Norwegian Data Protection Authority 2015, p.46.

[803] The code could also be, sometimes, executed on their servers.

[804] Eg network addresses used to address data packages. Eg 'Criterion A' in Article 29 WP (WP 194) 2012, pp.2–3; cf Article 8 in European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[805] See Article 10 of European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017; interestingly, Apple as a provider of Safari browser already introduced this functionality and plans to go even further, Slefo 14 September 2017.

It should be noted that the advertising industry and, independently, some software providers have introduced initiatives enabling some form of control from tracking, but they are not likely to be successful. The initiatives of the advertising industry, described in detail in Chapter VI, rely on opt-out mechanism and pertain only to third-party tracking. However, opting-out from third party tracking is quite difficult to manage. This is because those who opted-out need to be later recognised by each advertising server. So, for the opt-out functionality to work, data subjects need to be first identified (so, tracked) by those services just to opt-out from tracking. Taking this into account, an opt-in regime seems to be more intuitive (although it involves changing the way industry currently operates). Furthermore, with the initiatives introduced by the software providers (application Disconnect,[806] browser plug-in AdNauseam[807]), additional mechanisms which could help the users in this respect are being blocked by gatekeepers (such as Google) most probably because they interfere with their vision of 'data economy'.[808] There is some market potential for such solutions, which may be illustrated by the success of relatively similar web browser plug-ins called adblockers (filtering out advertisements),[809] which were called "the biggest boycott in human history".[810] Such tools securing data subjects from third-party tracking do not rely on service providers and this is why the regulation of software providers to introduce them (as stated above) is so important.

So, securing data subjects from uncontrolled tracking is necessary. While tracking by service providers should be controlled by PMM, third-party tracking should be screened on the level of user device.

C Conclusions

This chapter has explained how to implement PMM in the market. It has described a set of measures for influencing 'data markets' towards effectiveness in privacy management and

[806] See complaint of Disconnect (Case COMP/40099) 2015, p.63.

[807] Cox 18 January 2017.

[808] The anti-trust case before European Commision is still open, Commission issued a Statement of Objections in April 2016.

[809] Adblocks are used by 11 per cent of the world population on 615m devices with 30 per cent of yearly growth, PageFair 2017.

[810] Searls 29 September 2015.

effectiveness of their operations. The main measures rely on enabling users to employ Personal Information Administrators to support them in managing their data. To that end, PIAs should provide data subjects with a platform (software tool) which integrates the management of personal data in the ICT systems of a number of service providers via their Application Programming Interfaces. In this way, data subjects would have a one-stop shopping tool from which they could comprehensively manage their online privacy. PIAs should also be conveniently integrated into initiation of any personal data relationship between data subject and a new service provider, and should provide expertise in renegotiating the terms of such contracts. By doing all of this, they can be instrumental in increasing data subjects' awareness of data transactions. Such a correction of a business model of online services should be accompanied by other measures, such as data portability, and shielding individuals from uncontrolled tracking.

The main advantage of this scenario is that it does not presuppose changing either current business models of the service providers on the market, or personal data flows. So, it is possible to move smoothly from current online services to a human-centred model. But, it should be implemented by the means of architectural and legal regulatory methods. Architectural methods necessary to implement the PMM are expressing privacy preferences and policies between parties (users, PIAs and service providers), organisation of data and data types into a transparent and understandable structure, and providing enforcement and accountability. Their feasibility and, to some extent, design are discussed in the next chapter.

VI Architecture of Privacy Management

The previous chapter has presented how to implement PMM in the market with the help of Personal Information Administrators. They support data subjects in managing their personal data in the ICT systems of service providers. This can be achieved only by the means of technological tools. As discussed in Chapter IV, however, technology is not just the implementation of legal measures, but a separate tool, the 'code', which should shape online architecture to achieve balance in the relationships between data subjects and online service providers. This is important because, as noted in Chapter III, regardless of the legal mechanisms involved, the architecture of online services is the source of the imbalance of power. So, the countermeasures should also be architectural and enable individuals to make choices currently disabled by the architecture. The discussion below presents these countermeasures and verifies that the PMM model is feasible to implement in technology.

The architectural countermeasures needed to implement PMM should consist of two broad groups, which collectively cover supporting data subjects in exercising informational self-determination. They are shown in Figure 19 below.[811]

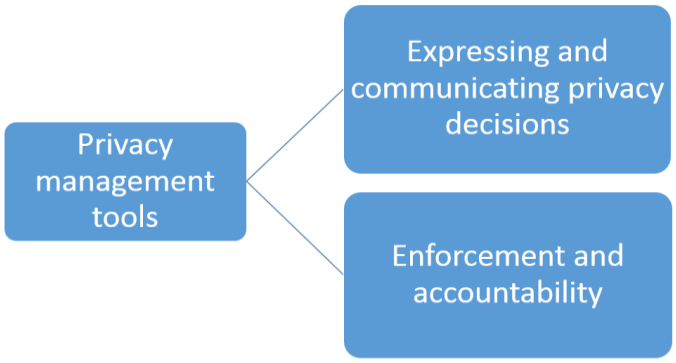


Figure 19 Types of privacy management tools

Firstly, the technology should enable data subjects to express and communicate their privacy decisions, which make up their privacy policies in the PMM. This cannot be done without organisation of personal data and their uses. Therefore, Part A below presents the ways to express privacy decisions by the means of ICT systems and Part B puts forward the proposition for organisation of data and data uses and discusses the way it should be presented to data

[811] Cf Le Métayer 2016, p.397; broader about technological tools, Koorn and others 2004; META Group 2005; Fritsch (D21) 2007; London Economics 2010.

subjects. Secondly, enforcement and accountability tools (discussed in Part C) deal with the problem of monitoring data in the ICT systems of service providers. That is to say, enforcement tools ensure that privacy decisions of data subjects are respected, while the accountability measures demonstrate that obligations of data controllers are met. In this area technology has its limitations and needs to be complemented by legal tools supporting accountability.

A How to Express and Communicate Data Subjects' Privacy Decisions

Privacy decisions need to be expressed in some policy language capable of being recorded in computer systems and conveying their meaning along the path of management data (ie from data subject through PIA to service provider). Many such languages already exist, so section 1 aims to find the best one for PMM. Then, section 2 discusses existing initiatives in which service providers are giving their customers some privacy management tools. Both sections show what can be done to transform data subjects' decisions into a set of understandable rules about handling their data.

1. *Privacy policies and policy languages for PMM*

Is there a technological standard which could be taken 'off the shelf' to implement individual privacy policies of PMM? Such an individual privacy policy expresses privacy preferences of the user[812] in a given policy language. Those preferences should be conveyed by the means of PIAs to service providers who collect and use personal data. This path is shown in Figure 20.

[812] Some authors discern privacy preferences of the users from privacy policies of the service providers. In this thesis, they are both called 'privacy policies'.

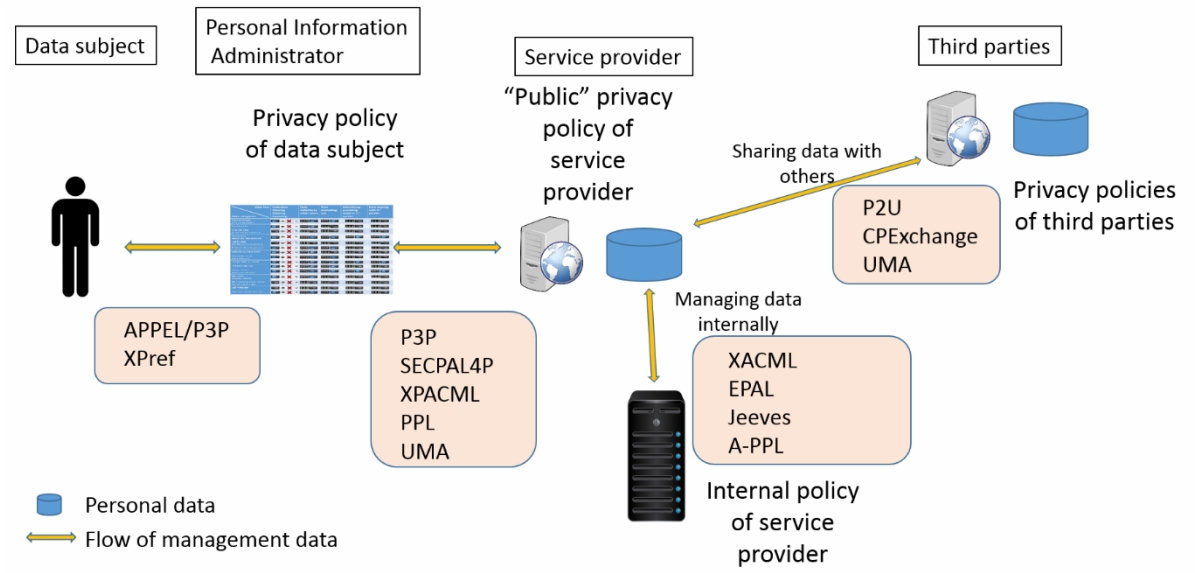


Figure 20 Privacy policies and languages to express them

In the orange rectangles, there are examples of existing technological tools (protocols or languages for privacy preferences) which may be used to formulate and communicate privacy policies in different relations (eg data subject to PIA). The common denominator for those technologies is that "they provide the means for stating what should be done in which sense with the data under consideration".[813] Figure 20 shows a number of steps to implement and enforce privacy policy. First, it needs to be formulated by the individuals themselves. Second, it needs to be communicated to the service provider. Then, the service provider needs to implement such policy within own ICT systems. Finally, it is also possible that such policy will be communicate further to third parties (eg subcontractors) if data are shared with them.

As illustrated in Figure 20, there are many languages (or protocols) to communicate privacy policies, but there is, so far, no common technology which enables such communication on a full path of data use.[814] Also, privacy policy languages available at the data subject's end lack capability to specify or configure enforcement mechanisms at the service provider's end.[815] So, there is no off-the-shelf standardised solution for PMM. The reason is that for each actor privacy policies fulfil a slightly different role. For data subjects, they allow them to express

[813] Kasem-Madani and Meier 2015, p.15.

[814] Technology reviews: Kumaraguru and others 2007; Ven and Dylla 2016; Camenisch, Fischer-Hübner and Rannenberg 2011, p.295.

[815] Hilty and others 2007, p.532.

their privacy preferences,[816] while for service providers those tools serve more to control and protect access to the personal data. This is because they are a valuable asset and because such protection is required by data privacy laws. Another problem is that policies created for individuals have to be written in an easy, understandable form, while conveying complex privacy meaning and context. For businesses, they need to clearly define the rules of conduct with data in their systems. This is the reason almost all those languages are machine-readable, and almost none are easily understandable by humans.[817] In the PMM 'business model' PIAs should bridge these gaps. Their role is to reconcile the views of data subjects and service providers and deal with these differences. Furthermore, the options they provide their customers (data subjects) with will determine the success of their businesses.

It is also useful to examine the well-developed approach to communication of privacy policies across the management data path – Platform for Privacy Preferences (P3P). P3P is a technical standard for communicating the privacy policies of a website to those who use it.[818] This is the same relationship as PMM, but P3P does not offer management of data in the ICT systems of service providers. The goal of P3P is to express web privacy policies in a standard format that can be retrieved automatically and interpreted by the software integrated into an Internet browser. So, it was designed to inform users of privacy practices of the websites and, by doing so, to make users more 'data sensitive' and make privacy a competitive factor which is similar to what is proposed in this thesis. P3P achieved a status of industry-wide standard of the World Wide Web Consortium (W3C) implemented into World Wide Web (WWW) technology.

Unfortunately, the implementation of this standard was unsuccessful, but its failure may give insight about the obstacles to overcome. There were a few underlying reasons for this failure. Firstly, P3P appeared to be too complex to be practical.[819] As a result, most people faced with its complexity were lacking the capacity to overcome it.[820] Furthermore, the aggravating factor was that P3P's protocol responsible for defining rules by data subjects (APPEL) contained

[816] And, therefore, some authors call them 'data handling preferences', Bournez and Ardagna 2011, p.296.

[817] Ven and Dylla 2016, p.174; Lazaro and Le Métayer 2015, p.24; Bournez and Ardagna 2011, p.312.

[818] W3C (P3P) 2007.

[819] Which was only partially addressed by the introduction of compact policies, Cranor and others 2008, p.275; Raggett 2010.

[820] Beatty and others 2007, p.69.

some errors.[821] Secondly, there was a lack of an appropriate feedback mechanism informing web users about the results of their actions. That is to say, implemented mechanisms were either giving no feedback at all (in Internet Explorer 6) or merely coloured-based feedback giving the result of policy comparison (plug-in 'PrivacyBird').[822] It seems that it was hard for users to understand the exact impact the colours of privacy icons had on their privacy.

Thirdly, businesses were clearly lacking incentives to adopt P3P.[823] In this respect P3P did not provide mechanisms to ensure that user preferences or decisions were respected by the service providers in their actual practice.[824] Without such insight into ICT systems of service providers the market mechanism, which was supposed to rule out untrustworthy service providers, could not work properly. Furthermore, as pointed out by Greenleaf as early as 1998, the user could not do anything about breaches of the P3P rules by service providers, so it was legally meaningless and "could only be little more than a framework for deception".[825] The same conclusion was described 12 years later, after an unsuccessful implementation of P3P by Cooper. She claimed the crucial problem was the lack of regulation: "companies had little reason to do so [express how they handle user data], preferring to protect themselves from the liability associated with revealing potentially unsavoury practices".[826]

To sum up, there is no off-the-shelf solution for expressing privacy preferences. But, it seems that there are all the tools necessary for PIAs to implement all the required functionalities. The lessons learned in the failure of P3P show that privacy management should be better in several ways. In relation to data subjects it should cover all services (not only web-based) and be simpler to use. In relation to service providers, it should be extended to provide data subjects with actual control over data and feedback about results of their actions. The incentive structure for companies also needs to be changed, which means that legal regulation is needed to implement it.

---

[821] Agrawal and others 2005, p.809; Li, Yu and Anton 2006, p.2.

[822] Beatty and others 2007, p.69.

[823] Cooper (RFC 6462) 2012, p.12.

[824] Diaz, Tene and Gürses 2013, p.943.

[825] Greenleaf 1998, p.615; similarly, Lessig ("The Law of the Horse: What Cyber Law Might Teach") 1999, p.521.

[826] Cooper (RFC 6462) 2012, p.12.

2. *Other initiatives allowing individuals to express their preferences*

As the previous section has shown there is no technological standard which could fully cover expressing privacy policies required by PMM. But, there are initiatives of the online industry which aim to recognise importance of data subjects' privacy preferences to a different extent. Reviewing them in this section gives a practical perspective of what has already been done in expressing privacy decisions and what is possible in this respect.

(a) 'Do Not Track' technology

'Do Not Track' (DNT) technology is a simple way to convey information to the web server that a user does not want to be tracked. The mechanism itself was put into the HTTP protocol[827] (technology used for viewing websites) and implemented by web browsers such as Firefox and Safari as early as 2011. It is hard to imagine a more straightforward mechanism, because the web browser simply sets DNT 'flag' to 1 and sends this to the service provider to signal this privacy requirement (or 0 to indicate otherwise). However, that changed nothing in the behaviour of service providers. This is because it was considered as not being a standard and there was no agreement as to the description of what exactly they should do in response to receiving such signal. The working group created by W3C worked very 'thoroughly' over five years and provided the standard recommendation in August 2015. And, surprisingly (or not) this standard "does not define requirements on what a recipient needs to do to comply with a user's expressed tracking preference, except for the means by which such compliance is communicated".[828] How the websites (including service providers) should react to receiving a DNT message was described in another standard which was finally defined in April 2016.[829]

That 2016 standard, called 'Tracking compliance and scope', perverts the meaning of the words 'Do Not Track'. Firstly, the positive signal about compliance means that service providers actually *may* collect, retain and use data received from those users "customizing

[827] As so-called 'extension'.

[828] Section 1 "Introduction", W3C (DNT) 2015.

[829] W3C ("Tracking Compliance and Scope") 2016.

content, services and advertising with respect to those user actions".[830] It is only third parties that should not do this. So, 'do not track' means only 'do not track by third parties'.[831] Even for third-party tracking there are a number of exceptions, including that the customer has consented.[832] This is surprising, because consent (presumably a prior one) is used as a waiver to subsequent lack of consent (signalled directly in request by DNT 'flag'). Secondly, similarly to P3P, there is completely no mechanism for the user to verify or check the behaviour of the website.

So, the DNT mechanism was substantially delayed and its effectiveness diminished to blocking some of the third-party tracking, and, like P3P, it was simply not implemented by the biggest service providers.[833] Once again the market mechanism drove privacy out according to the Copernicus (Gresham) law.[834] This example shows that even the simplest way of signalling privacy needs to be implemented with the support of the legal regulatory mechanism.

(b) One-stop shopping opt-out tools

There are a number of self-regulatory initiatives used by advertiser organisations which (allegedly) aim to provide customers with opt-out from behavioural advertising. The best known seems to be 'Your online choices'.[835] It was one of the actions undertaken before the adoption of the law regulating some aspects of using tracking tools in Europe.[836] Such tools aim to give customers a one-stop shop website to opt out from tracking by any participating advertising brokers. The problem at the heart of this idea is that in order to be counted for opt-

[830] Section 3.2, W3C ("Tracking Compliance and Scope") 2016.

[831] Which seems to be close to the Orwellian 'no animal shall sleep in a bed with sheets'.

[832] Section 3.3, W3C ("Tracking Compliance and Scope") 2016.

[833] There are just nine companies supporting DNT (as of 1/11/2017), Future of Privacy Forum n.d.

[834] Eg Akerlof 1970, p.488; for example, DNT was supported by Twitter for some time, Libert 2015, p.8; but later Twitter declared that the lack of 'industry adoption' made them discontinue honouring DNT, Twitter n.d.

[835] "Your Online Choices – EU" n.d.; "Your Online Choices – AU" n.d.; "Your Online Choices – NZ" n.d.; there are also others, eg NAI: Network Advertising Initiative n.d.; Digital Advertising Alliance n.d.

[836] Directive 2009/136/EC of 25 November 2009, Article 2(5), which amended Article 5(3) of ePrivacy Directive.

out, individuals need to *enable* tracking in their browsers (to be tracked as those opting-out).[837] This is "misleading at best and deceptive at worst", because individuals need to resign from their own tracking protection tools to be able to use it.[838]

These tools have also other problems which seem consistent with the lack of incentive of their providers – their functionality erodes over time. For example, the structure of the European 'Your online choices' website changed so the user had to choose a particular country in which it operated rather than opt out from advertising in all of them.[839] Also, the opt-out mechanism is now hard to find among additional 'useful' information. Over the years, the number of participating advertising networks have decreased and most of them nowadays seem to not offer the opt-out functionality at all – they permanently have the status 'currently unconnected'. While similar tool of Network Advertising Initiative seems to be more 'alive', it represents only a small part of the advertising business.[840]

But, notwithstanding all those problems, those initiatives show that managing privacy from a single panel across multiple computer systems providing different services from different providers is, indeed, possible. They not only prove that expressing privacy choices is possible, but also that it is possible on the industry-wide scale. However, similar to P3P and DNT, it is useless without accountability and enforcement.

(c) Privacy dashboards

The biggest online service providers, like Facebook or Google, go slightly further than simple opt-out tools and implement user interfaces (UI), so-called 'dashboards' providing individuals with an ability to express more complex privacy decisions.[841] Dashboards seem to be an equivalent to what is needed to implement PMM, because individuals can decide how particular service providers handle their data. However, they have significant shortcomings as

[837] So, the opt-out tool requires unblocking third-party cookies, Digital Advertising Alliance n.d.

[838] Libert 2015, p.7.

[839] As of February 2017. Also, the Australian 'Your Online Choices' website disappeared from the Internet, while the New Zealand one never had an opt-out engine.

[840] 99 companies as of February 2017.

[841] Betkier ("Individual Privacy Management") 2016, pp.330–332.

they are not built to deliver functionalities of privacy management. In this respect, the biggest problem seems to lie in the organisation of data and data uses. So, dashboards do not give a comprehensive view of all data and their uses but only some aspects of service providers' activities. Usually, there is little to show users about how service providers use their data on the other side of the market where they are for sale. For example, the research of 'traceability' (ie the relationship between T&Cs and privacy controls) found that only 15–25 per cent of privacy policy statements were covered by controls in a consistent and unambiguous way.[842] The remaining T&C statements were either imprecise or ambiguous, or completely 'broken', so that the 'traceability' did not exist.

This problem could be explained by the following example relating to Google and location data. The firm presents the users with an option to "[m]anage your Google activity" in which it is possible to "[t]ell Google which types of data you'd like to save to improve *your* Google experience".[843] By the means of "[a]ctivity controls" it is possible to "control what data *gets saved to your Google Account*" to "make Google services more useful *to you*". Within those controls there is a "Location History" (both words beginning with uppercase) which can be turned off and on. It remains an open question what happens when the user switches it off. The average user's perception is probably that it stops Google from collecting and using one's location data.[844] This perception may be amplified by the fact that those data can be removed from the map presented in the background. But, neither the expressions cited above nor additional support information[845] says this. They simply give individuals control over something defined as "Location History" used to shape their experience with Google products. But, whether Google continues to collect location data and how those data are used for goals others than adjusting Google products to the user seems to remain out of the scope of this tool. Furthermore, the collection of location data and their use with their business partners (eg to profile those individuals) is completely compatible with Google's Privacy Policy, which states explicitly that Google may collect and process information about location for providing its services.[846] This is contrary to the perception of the users who switch off their "Location

[842] Anthonysamy, Greenwood and Rashid 2012.

[843] Google ("Personal info & privacy") n.d. As of September 2017. Emphasis added by the author.

[844] Eg Steele 20 April 2017.

[845] Cf Google ("Manage or delete your Location History") n.d.

[846] Google ("Privacy Policy") n.d.

History". So, without clear, fixed organisation of data and data uses it is not possible to move on with privacy management.[847]

In the absence of such data organisation controlling will inevitably be imperfect. This is because individuals do not really know what they control. Privacy settings are also too fragmented and scattered throughout different categories along with other settings to make them effective. Similarly, monitoring is difficult, because there is no information about data uses. In the case of Facebook, it is possible to download data and make some inferences which friends they were 'shared' with, but there is no information about the data uses by Facebook itself. The same problem also makes planning a difficult task. Planning is further affected by the fact that T&Cs and dashboards change often and in a substantial way. It is simply not possible to plan data and data use when they change several times a year. [848]

Having said that, dashboards demonstrate that much of the PMM could be implemented.[849] Firstly, they present user interfaces (UI) accessible for individuals in which they can have a say about particular uses of data. Secondly, this interface is a single point of access to the complex, closed systems of service providers. Thirdly, they give some access to raw data, for example by means of downloading Facebook activities or Google search history, or by presenting location data on a map, like in the example of "Location History" above. If those functionalities are achievable over UI, there should be no problem with providing them over application interface (API) through which PIAs could manage privacy settings for the data subjects. But, first, the privacy settings should take into account interests of those data subjects.

To sum up, the main obstacle preventing individuals from achieving better control over their data through self-regulatory initiatives are, again, the market forces which drive privacy out. In the case of DNT the lack of incentives for service providers was seen in a blatant way because the service providers did nothing for five years. But, one-stop shopping opt-out initiatives from advertising alliances show that access to a set of standardised choices in

[847] Also, example about Facebook, Betkier ("Individual Privacy Management") 2016, p.331.

[848] Eg Google policy changed 11 times in 2015–2017, Google ("Updates: Privacy Policy") 2017. More details in the next chapter.

[849] Similarly, Betkier ("Individual Privacy Management") 2016, p.332.

multiple services (as via PIAs) is possible. Furthermore, privacy dashboards show that technology to give individuals access to more complicated privacy settings through UI, together with access to their data is already in place. So, it seems that technology can deliver the PMM functionality allowing access to data and making decisions about them. However, the privacy choices need to be better organised and aligned to the interests of individuals. It is time, now, to show how data and data uses should be organised.

B How to Categorise and Present Data and Data Uses

As explained above, the organising function, having the system organised for privacy management, is crucial to implement PMM. This Part attacks the nub of this problem by proposing the categorisation of data and data uses. In this respect, the thesis does not consider physical data organisation (ie databases, physical locations, and physical data structures), but shows (in section 1) a logical structure: how data are logically organised in categories. Then, in section 2, it shows how data choices should be presented to individuals.

1. *Categorisation of data and data uses*

In order for PMM to work, types of data and data uses need to be understood in the same way by both data subjects and service providers. This is, in part, a problem of transparency of service providers because they do not disclose what data they have and what they do with them. Solving this problem is crucial for rational decision making and accountability.[850] But, transparency should not just disclose data in the ICT systems of service providers, because nobody would understand this. Instead, it should give access to information about them comprising "veridical, meaningful, comprehensible, accessible, and useful data".[851] This information needs to be *produced* on the base of accessible data and be coherent with the business logic of internal systems of service providers. This information will be a base for data subjects to make decisions about their data and data use. Following those decisions it should

[850] It underpins accountability, safety, welfare, and informed consent, Turilli and Floridi 2009, p.107; similarly, Spiekermann 2015, p.59.

[851] Turilli and Floridi 2009, p.108; similarly but more broadly, Spiekermann 2015, pp.59–61; also, "we do not want to look through, but look directly at", Menéndez-Viso 2009, pp.161–162.

allow service providers (their ICT systems and employees in the back-office) to distinguish particular data and their uses from other categories to treat them in a way specified by data subjects.

(a) Categories of data

Data categories are usually determined by businesses and vary across different service providers. So, there may be different data categories in social media,[852] search services, navigation systems, financial systems, etc. On the surface, it seems very hard to reconcile those categories to build a common data hierarchy. However, when one looks more clearly at data organisation it can be seen that some data categories are either derived from their origin or function (eg location data, web searching data), or from the existing legislation (eg traffic data, location data)[853] which is also usually based on the origin or function of data. Such organisation (categorisation) should be maintained across the whole ICT system to allow for specific treatment of particular data.

The techniques for doing this are already in use by service providers. For example, the International Association of Privacy Professionals (IAPP)[854] advises service providers to create classification rules for data.[855] Having data classified according to the level of responsibility of data controllers (which should correspond to sensitivity of data) allows data controllers to protect data by corresponding access control systems within their internal ICT environment. IAPP also advises not introducing more categories than imposed by regulation.[856] This is sensible advice, as it tells service providers to include only such complexity as required. However, this approach takes into account only the perspective of service providers, while their customers may have different ideas about revealing data which have assigned the same levels of access control. For example, health and financial data may

[852] Additionally, in social media personal data are published by data subjects themselves, but those data are considered as controlled (to some extent) by the individuals who publish them and are not in the scope of this thesis. So, if one social media user publishes personal data of another, they should use existing mechanisms to resolve the conflict.

[853] ePrivacy Directive, Article 2.

[854] "International Association of Privacy Professionals" n.d.

[855] Cannon 2014, p.36.

[856] Ibid., p.36.

be on the same (higher) level of sensitivity but may be treated differently by data subjects. Therefore, classification rules should include data subjects' perception.

As a result of analysis of different categorisations[857] it seems that the best approach is to apply relatively simple thematic division of categories. So, instead of defining a set of details related to, for example, credit card (eg name, number),[858] all of them should be put in a more general class of credit-card data or even financial data.[859] This may allow service providers to keep the relation (mapping) of data to their sources (eg data from payment application are financial, data from heart sensor are health data) and also give data subjects some estimation about the sensitivity of particular data type.[860] For example, Kelley and others started with P3P terminology, but found it too complicated, so they scaled it down to 10 categories of data. Those 10 categories were related to websites only, so there is a need to apply a slightly broader approach. Such an approach has been found in a draft of a standard by the Kantara Initiative called 'Consent Receipt Specification'.[861] The idea behind this standard is to provide users with a record of each consent in a standardised way so it can be easily tracked, monitored or managed.[862] They aim at increasing the level of transparency and data-awareness of data subjects which is consistent with PMM.[863] 'Consent Receipt Specification' proposes 15 categories listed in Table 4.[864]

Table 4 Proposal for data types/categories, following the Kantara Initiative.

	Data Category	**Description**
1	Biographical	General information like name, date of birth, family info (mother's maiden name), marital status. Historical data like educational achievement, general employment history.
2	Contact	Address, email, telephone number, etc.

[857] W3C (P3P) 2007; Wacks 1993, p.230 ff.; Kelley and others 2010, p.3; Betkier ("Individual Privacy Management") 2016, p.326; Lizar and Turner 2017.

[858] Eg s 5, W3C (P3P) 2007.

[859] Bournez and Ardagna 2011, p.299; also, P3P data types, s 3.4, W3C (P3P) 2007.

[860] The approach to define sensitivity on the lower level seems to be overcomplicated, eg Wacks 1993, p.230.

[861] Lizar and Turner 2017.

[862] Ibid., p.3.

[863] Although insufficient, see Chapter V.

[864] Appendix A, Lizar and Turner 2017, pp.22–23.

3	Biometric	Photos, fingerprints, DNA. General physical characteristics – height, weight, hair colour. Racial/ethnic origin or identification.*
4	Communications/ Social	Email, messages, and phone records – both content and metadata. Friends and contacts data. Personal data about self or others.
5	Network/Service	Login ids, usernames, passwords, server log data, IP addresses, cookie-type identifiers.
6	Health	Ailments, treatments, family doctor info. X-rays and other medical scan data.
7	Financial	Information like bank account or credit card data. Income and tax records, financial assets/liabilities, purchase/sale of assets history.
8	Official/Government Identifiers	Any widely recognised identifiers that link to individual people. Examples include National Insurance, ID card, Social Security, passport and driving license numbers, NHS number (UK).
9	Government Services	Ie Social Services/Welfare – Welfare and benefits status and history.
10	Judicial	Criminal and police records, including traffic offenses.
11	Property/Assets	Identifiers of property – license plate numbers, broadcasted device identifiers. Non-financial assets. Could include digital assets like eBooks and digital music data.
12	Employee Personal Information	Records about employees/members/students not elsewhere defined. Including HR records such as job title, attendance/disciplinary records. Salary – as opposed to income.
13	Psychological/ Attitudinal*	Including religious, political beliefs, sexual orientation, and gender identity* – though not genetic gender which is Biometric. Traits and personality measures or assessments, but not psychological health – which is health data.
14	Membership	Political, trade union affiliations, any other opt-in organisational/group membership data – third party organisations only. Includes name of the employer when not

		held by the employer. Could extend to online platform membership. Some might be more sensitive than others – may require a separate category.
15	Behavioural	Any data about the behaviour, habits or movements of an individual – electronic or physical. Location, browser/search history, web page usage (analytics), energy usage (smart meters), login history, calendar data, etc.

* - there seems to be some inconsistency in putting different types of identity characteristics in different categories. In the author's subjective opinion they all should be placed in category no 13 under a different name, more reflecting their sensitive character;

This proposal of the Kantara Initiative is a very good high-level description of data types for PMM. This standard defines the concise set of categories which service providers would have to offer for data subjects to manage. It seems it has adopted a compromise which strikes the balance between readability, and internal and external coherency of categories. Those categories of data do not necessarily have to be collectively exhaustive, so new ones may emerge in future. It is also possible to create more fine-grained subcategories which could be managed independently. For example, behavioural data representing data collected by tracking individuals' moves could be split further into location data, search history, activity within the service, data collected by the means of sensors, etc. Nevertheless, there should be some common standard of data types and this seems to be a good base for such a standard.

(b) Categories of data use

Defining types of data use is also difficult, but, similar to defining types of data, can be achieved on a general level. There may be different uses specific to different types of online businesses. So, regulation relating to disclosing data to third parties rarely specifies any particular uses. On the contrary, it is rather generalised and directed to keep those uses within limits disclosed at the time of data collection (so-called 'purpose specification' principle).[865] This is because another approach which aims to declare all possible 'purposes', such as in P3P schema, would be extraordinarily complicated.[866]

[865] See the next chapter.

[866] 12 different purposes additionally extended in 1.1 version of P3P by 23 'primary purposes', s 3.3.5 of W3C (P3P) 2007.

Instead, defining types of data uses should give data subjects simple but meaningful options. Such options, as noted earlier in the thesis,[867] should be based on the level of risk introduced by data processing. The idea for devising such a categorisation comes from the method of presentation of data sensitiveness and major data uses by the Boston Consulting Group.[868] They discerned for the purpose of their analysis of value of personal data only four categories of data use: delivery of requested service, enhancement of services, transfer to third party (anonymised), and transfer to third party (traceable). Those two last categories pertain to (respectively) providing third parties with personal data enabling them to reach the data subject with advertisements ('a sales lead'), and to passing their personal data to third parties. This could be also used for PMM. However, as mentioned in Chapter II, there is a need to add data use related to the automatic profiling[869] of data subjects.[870] Profiling should be left for data subjects to decide, because it increases the level of risk for them. Also, marketing and marketing with profiling are substantially and, for data subjects, noticeably different. So, the final proposal for categories of data uses is presented in Table 5.

Table 5 Proposal for data use categories

	Use Category / Purpose	Description
1	Own use necessary to provide the service	Use for activities strictly necessary to provide service, including elements like processing payments, service delivery (also by means of a third party who does not collect personal data for other purposes).
2	Own marketing use	Use for marketing activities related to service extension or other services in which data subject may be interested.

[867] In Chapter II.

[868] The Boston Consulting Group 2012, p.51.

[869] As defined in Chapter II, profiling is the use of personal data to evaluate certain personal aspects relating to a natural person.

[870] There is some degree of flexibility between types of data and data uses. For example, BCG recognised data types basing on the 'prevalent method of collection', so as a result data could be tracked or profiled (mined). Here tracked data are in 'behavioural' type of data, while profiling is understood as type of *data use*. But, recognising 'profiled/mined' type of data is just an alternative way of seeing this. Cf The Boston Consulting Group 2012, p.57; cf Betkier ("Individual Privacy Management") 2016, p.326; but, data uses, Kelley and others 2010, p.3.

3	Profiling	Use for profiling data subject.
4	Providing leads to third parties (anonymised transfer)	Use for providing third parties with data allowing contact with data subject to deliver their offers and services (also for communicating to data subject the offers of third parties).
5	Providing data to third parties	Revealing data to third parties, including publishing them.

Similarly to data categories, data use categories can be extended or split into more fine-grained choices. However, the categories showed in Table 5 seem to be a good base for a standard as they seem to be meaningful for both data subjects and service providers.

So, to sum up, the 'ontology' of data and data uses can be defined on a higher level of abstraction to present the customer with simple options. To implement PMM in technology there is a need to start with some schemas and the ones presented in this section seem to strike a good balance between comprehensibility and readability. Additional complexity, if required, may also be added by creating a hierarchy of data and data types below the presented main categories.

Knowing the categories of data and data uses it is time to show how they should be presented to data subjects.

2. *Presentation of choices to data subjects*

Presentation of the categories which have just been described to data subjects is very important because it needs to enhance their level of information and understanding (or minimise information asymmetry) and help them to make informed decision about data.[871] As mentioned in Part A, improper presentation was an element of failure of P3P.

[871] Transparency Enhancing Technologies (TETs) in Future of IDentity in the Information Society (FIDIS D7.9) 2007, p.49; minimising information asymmetry may be also seen more widely as a whole set of prevention, avoidance, and detection tools, Jiang, Hong and Landay 2002, pp.183, 187.

As well as achieving simple categorisation of data and data uses, it is possible to achieve a clear presentation of them to individual users. There are well-developed ideas to present privacy policies in a few layers: standardised privacy icons[872] or a short table, a standardised short text version, condensed versions,[873] and a full version readable for lawyers.[874] The most promising visualisation can be found in the project of 'privacy nutrition labels' (so called because of their similarities with food labelling) developed by Carnegie Mellon University.[875] Kelley and others developed some standardised formats with the help of focus groups and compared them in an online user study of 764 users.[876] The research has shown that a standardised table (as in Figure 21)[877] presenting holistic view of privacy policies conveyed the information of the privacy policies of the website in the most accurate way (73–90 per cent).

[872] Eg Holz, Zwingelberg and Hansen 2011.

[873] Centre for Information Policy Leadership and Hunton &Williams 2006, p.10 ff.

[874] OECD (DSTI/ICCP/REG(2006)5) 2006; Kelley and others 2010; Cannon 2014, pp.29–31; Bournez and Ardagna 2011, p.301.

[875] Kelley and others 2009; also, more developed version, Kelley and others 2010.

[876] Kelley and others 2010, pp.5–8.

[877] Ibid., p.3.

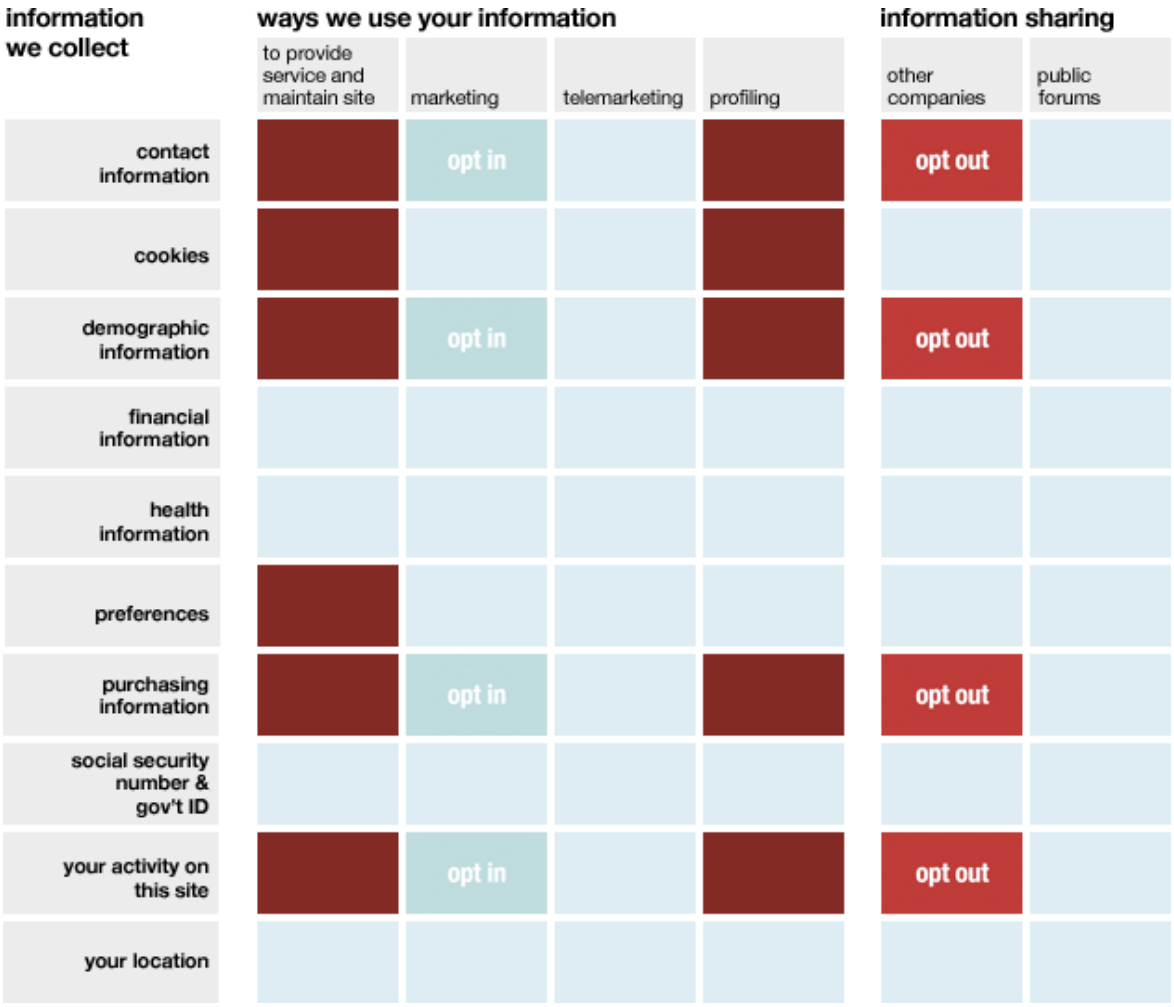


Figure 21 Standardised table version of privacy 'nutrition label'

In Figure 21, the data types are presented in rows and data uses in columns. This particular project was developed for web pages, so for PMM the types of data and data uses should be changed to those described above to convey the privacy decisions to a broader category of service providers. This could be done, for example, similar to the idea of user interface by the author presented in Figure 22:[878]

[878] This includes the categories from section 1. Cf Betkier ("Indvidual Privacy Management") 2016, p.326.

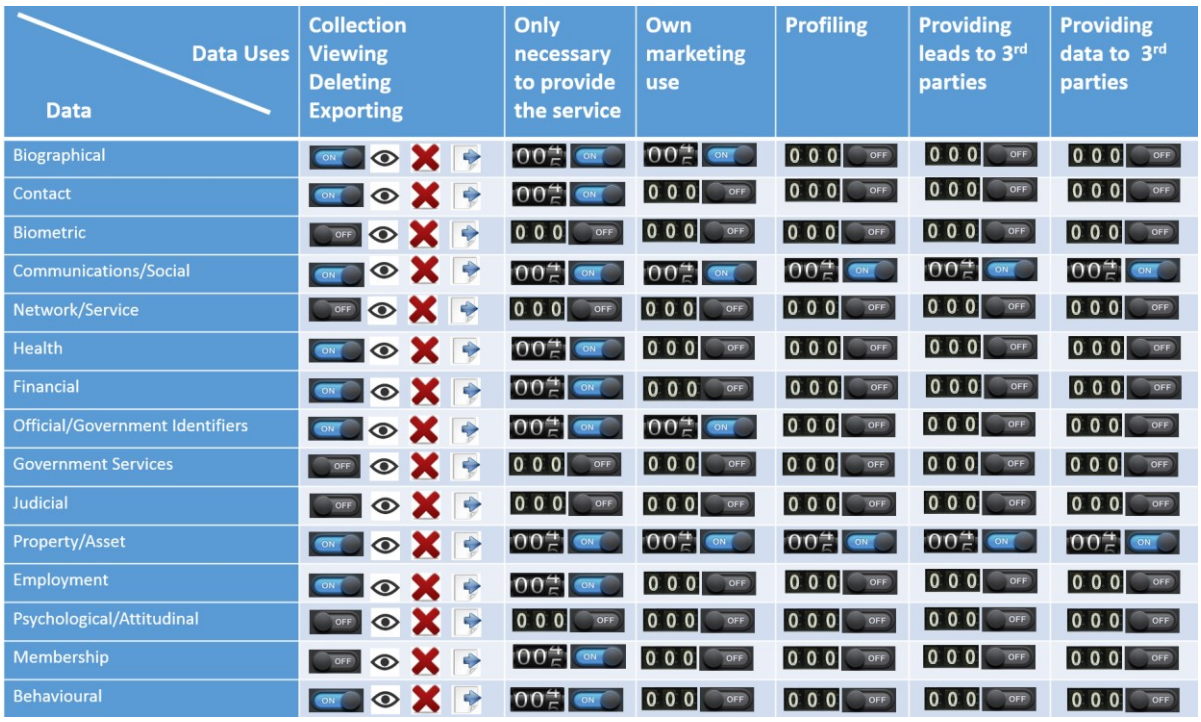


Figure 22 Individual privacy management interface

In this view, which also has the form of a table, for particular data categories users see some information about data use (conceptualised as a counter) and, additionally, control options (conceptualised as on-off switches and icons linking to forms allowing users to view, delete, or export data). Of course, design matters and some effort needs to be put to achieve simplicity and overall readability of the privacy controls as in the Carnegie Mellon project. However, it is entirely possible that the outcome of a standardisation project on the categorisation of data and data uses would be somewhere between these two presented approaches. It is possible that this view is too detailed and a simpler idea is needed, like, for example, in a 'strawman proposal' of Customer Commons.[879] This is not the place to present a definite view, but rather to show that this problem is possible to solve.

To sum up, ideas for achieving human readability of privacy settings central to the success of any PMM tool seem to go towards privacy icons or simple standardised tables which visualise data and data uses. The best of such data visualisations seems to be the 'Privacy Nutrition Labels' developed in Carnegie Mellon University. Based on this concept, it is possible to introduce developed types of data and data uses and privacy management controls which

[879] Customer Commons 2014. However, there are no privacy management controls there.

overall may be presented in a similar way. There are no conclusive answers to what such an interface should look like, but it can be relatively simple in design.

C How Technology Supports Enforcement and Accountability

What architectural tools are necessary to implement PMM functions in the ICT systems of service providers? Those systems should handle personal data in a way which respects individual privacy choices and protect those data against unauthorised use. Section 1 identifies technological tools already used by data controllers to implement privacy obligations and shows which functionalities need to be additionally developed to implement PMM. Then, section 2 deals with the much harder task of assessing feasibility of implementation of those additional functionalities.

1. *Technologies used to handle personal data in the ICT systems of companies*

There are existing practices which privacy-aware organisations use to handle personal data. They form a good foundation to build additional functionality enforcing privacy management. The best practices recognised by Bamberger and Mulligan in international research include 'managerialisation' of privacy, so integrating privacy as a core value into company goals and into its risk management and audit systems.[880] In this respect, first of all, organisations are required to care about personal data, so they need to identify and handle them appropriately in their day-to-day operations. This boils down to special treatment of personal data throughout the whole data lifecycle: collection, retention, use, disclosure, and destruction.[881] To manage privacy from a business perspective, firms need to introduce a data programme which, on collection, identifies data as personal, secures them and restricts access to them except for particular business purposes and scenarios (the same as communicated to customers).[882] For

[880] Bamberger and Mulligan 2015, p.177; also, Finneran Dennedy, Fox and Finneran 2014, p.35; or Pearson 2012, pp.222–225.

[881] Cannon 2014, p.57.

[882] Eg Cannon 2014, pp.57–79; Finneran Dennedy, Fox and Finneran 2014, pp.233–238; Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia 2012, pp.4–5.

the businesses, all this is needed to limit the risks bound up with using personal data: business risk relating to loss of customer trust and reputation, and the regulatory risk of being fined by the DPA (which may be also seen as a business risk).

The practices and technologies enabling such personal data programme include:[883]

- Preparing privacy policies which describe personal data handling procedures and limit their use;
- Identifying information collected, held, or transferred;
- 'Labelling' data – categorising them;
- Securing storage and access to data (eg encryption, a policy-backed access control);
- Keeping the track of personal data by logging – creating metadata about personal data use and third parties involved;
- Introducing a monitoring process to make sure that the privacy policies are enforced and regularly reviewed, which includes controlled introduction of new use scenarios (eg the so-called Privacy Impact Assessment), auditing, and incident handling.

These are shown in Figure 23.

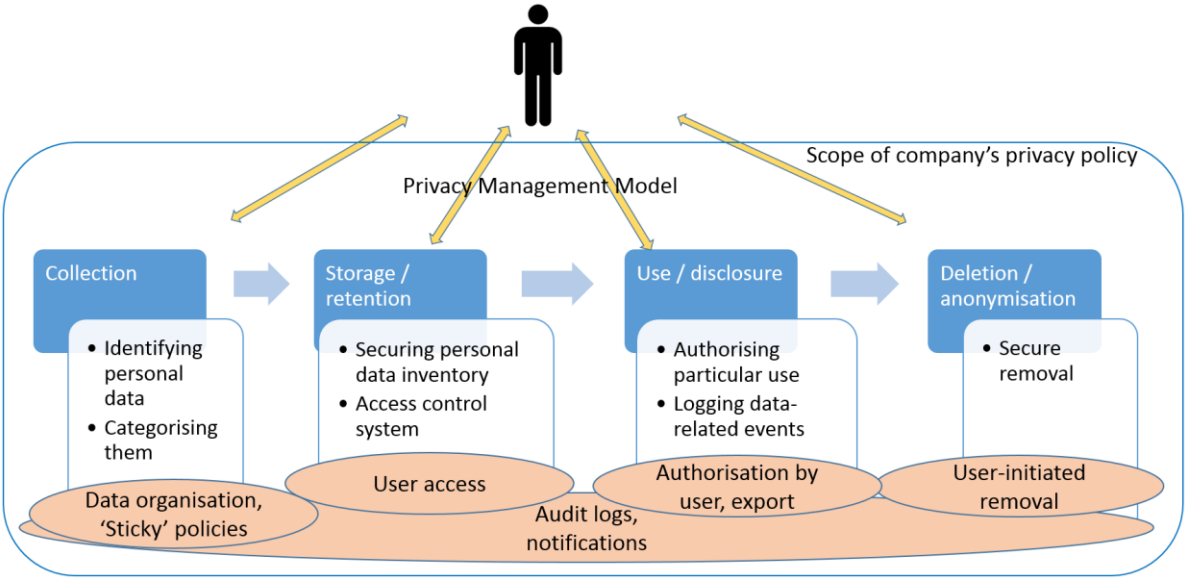


Figure 23 Technologies to enforce privacy management

Figure 23 presents the current privacy management technologies in white rounded rectangles and enhancements to current business environment necessary to implement PMM in orange

[883] Bamberger and Mulligan 2015, p.178; Cannon 2014; Finneran Dennedy, Fox and Finneran 2014, pp.54–55.

ellipses. Those enhancements are needed to ensure that privacy choices of individuals are respected in data processing. Some, like introducing standardised data organisation and access to data, have already been covered in Parts A and B. The following section discusses remaining technologies related to enforcement (such as 'sticky policies': attaching to data policies defining their permitted use) and technologies supporting accountability (eg access to audit logs and active notifications about privacy events).

So, this section has shown that the existing practices used to handle personal data in privacy-aware organisations are covering much of the functionality needed for the PMM implementation. Personal data are (or should be) treated according to the pre-defined policy, appropriately 'labelled' and tracked in the internal ICT systems, and access to them should be controlled by some policy-backed control mechanism. Service providers should also control personal data use, especially disclosure, storage, and deletion. To make such systems ready for PMM they need to be enhanced so they recognise standardised types of data and data uses (as defined above) and are enhanced through additional mechanisms which increase data subject participation in the business-oriented process. This also includes data subjects' access to the important functions monitoring enforcement of privacy policies and, therefore, enabling accountability.

2. *Enforcement and accountability tools*

In principle, enforcement of privacy management is weak, as data are processed out of the 'reach' of data subjects.[884] Without additional tools they cannot make sure that data controllers respect their privacy choices or privacy policy. As their systems remain out of control of data subjects and PIAs, no matter how complicated those technologies are, they can always be circumvented by a 'malicious' service provider.[885] This, however, should not undermine the sense of using them, but should rather put requirements to their design.[886] For example, the enforcement systems need to be constructed in a way which makes it obvious whether a given action constitutes a breach of rules and, therefore, prevent disputes over the possible

[884] D'Acquisto and others (ENISA) 2015, p.47.

[885] Bournez and Ardagna 2011, p.302.

[886] Le Métayer 2016, p.396.

qualification of privacy breaches as mistakes (false positives). Such an enforcement system would need to be complemented with trust, perhaps external auditing, and an accountability mechanism in which lack of adherence to the rules results in some negative consequences. Such mechanisms should be backed by the legal regulatory tools.[887]

Enforcement would not be possible in an open system like most of today's World Wide Web, but, it is, in principle, possible in the closed ICT systems of service providers where all users can be authenticated and their actions authorised.[888] In particular, it is technically possible to build an information system which keeps personal data in a central location and enforces privacy policies on access to them. Such systems have been described in the literature and are possible to build.[889] What may be problematic, however, is how to enforce privacy policies where data are distributed within a company or shared with another company (eg a subcontractor).

To overcome these problems, computer science has been directed towards a general concept of 'usage control', which aims to cover the whole lifecycle of data.[890] Its ideas seem to concentrate on guaranteeing that data policy stays associated with personal data even when data is conveyed to another subject.[891] The idea was presented in 2002 as the 'sticky policy paradigm'.[892] It was further extended to control access to confidential data by the means of a trusted third party,[893] and even to manage privacy across multiple parties.[894] The policies may be bound to data either 'weakly' by the simple association of a policy to data by an external system, or 'strongly' by using cryptography.[895] In the latter option, cryptography makes sure that only an authorised user with the respective key can have access to data. This gives a lot of flexibility for data management: access can be policy-based, fine-grained, and controlled by

[887] See next chapter.

[888] Cf enforcing "the right to be forgotten", Druschel, Backes and Tirtea 18 October 2011, p.8.

[889] Agrawal and Johnson 2007; He and others 2016.

[890] Term introduced by Park and Sandhu 2002.

[891] Le Métayer 2016, p.424.

[892] Karjoth, Schunter and Waidner 2002, pp.74–75; see also very similar concept of 'privacy tags' in Jiang and Landay 2002; also Bruening and Waterman 2010.

[893] Mont, Sharma and Pearson 2003, p.11.

[894] Pearson and Casassa-Mont 2011.

[895] Mont, Sharma and Pearson 2012, p.32.

the encryption mechanism.[896] Also, if a data policy is verified before data use by the means of a policy server it is possible to guarantee that changes in the data policy (eg revoked consent) are taken into account. All of this, however, does not prevent malicious users from sharing decrypted data[897] or the unauthorised copying of data by human observers (for example, by photographing the screen).[898] Technical solutions which could overcome these problems are under development, and there is significant effort being applied in this direction, but they seem to be still in the phase of proposals.[899]

If technology is not enough to enforce privacy management on its own, therefore trust and legal tools need to complement technical ones. Such solutions may be based on indirect control and holding service providers to account ex post for their actions. [900] To that end, technology may be helpful to show 'accounts' proving that the practice of data controllers meets their policies. This, first of all, may be the role of privacy-aware transaction logs.[901] Logging is simply writing to a file (called log) records of the events of specific type occurring in the ICT system. It may require more resources from such system (as additional operations are performed), but it gives additional, often crucial information needed to verify its operations in detail. In other words, the log file is an ICT equivalent of an 'account' which gives information on how data were handled, which may be used to determine whether a privacy policy was breached.[902] As demonstrated in a formal model by Butin and Le Métayer, it is possible to implement an effective accountability model without recording additional personal data.[903] However, this is not a simple task. It requires decisions made at the design stage, appropriate security measures ensuring integrity and confidentiality of the logs (against tampering), and an additional interface to make use of the logs to verify data operations.[904] Furthermore, it

[896] Pearson and Casassa-Mont 2011, p.64; see also Leng and others 2013.

[897] Le Métayer 2016, p.425.

[898] Druschel, Backes and Tirtea 18 October 2011, p.8.

[899] Eg Zuo and O'Keefe 2007; Kounga and Chen 2011.

[900] See Chapter IV.

[901] D'Acquisto and others (ENISA) 2015, p.43; Le Métayer 2016, p.427; Weitzner et al. 2008, p.86.

[902] Butin, Chicote and Le Métayer 2013; cf the critique of logging personal data uses in social networks on the grounds that it introduces additional surveillance, Sayaf, Clarke and Rule 2015. However, it pertains to publicly available data and not personal data use in the internal systems of service providers.

[903] Butin and Métayer 2014, p.177.

[904] Le Métayer 2016, p.429.

seems that (recently 'fashionable') blockchain technology may be of some support to accountability in this area.[905]

Moreover, logging may be extended by active mechanisms monitoring data flow and notifying users (or PIAs) about certain important events pertaining to their personal data. This would serve as a 'breaking the glass' procedure in case of emergency. An obvious application of such a feedback channel is an automatic notification about privacy breaches, but there are ideas to extend this mechanism to allow users to set their own level of notification according to their privacy policy.[906] In this way, such notification messages could be used as proof of accountability. This may be realised in 'push mode' as an extension of the logging service (records sent to a remote system rather than stored locally), or in a 'pull mode' as responding to a request of actively monitoring system of PIA.[907] Logging may be extended so that it allows for 'provenance tracking', allowing individuals to track the origin of their data.[908] There are, however, some privacy risks involved in tracking data, as it may reveal personal details of others. This may be the case, for example, with access to any input of raw data (eg from CCTV camera) or access to common metadata (eg system logs including data of others).[909] Therefore, provenance tracking may be a useful tool for showing the origins of data, but it should not actually show the data which are the source of the personal data in question.[910]

Finally, evidence of accountability can be taken from the ICT systems of service providers used for wholesale transactions with personal data. There has been a large shift in Internet advertising recently towards programmatic advertisement display.[911] Advertisement brokering systems now link the supply and demand platforms and conduct on-the-spot auctions of advertising place for particular users.[912] This means that the personal data of data subjects are being verified and sold 'on the spot' by publishers to whichever advertisers offer the best

---

[905] See more general view on accountability Herlihy and Moir 2016; also, more specifically Kosba and others 2016; project example, 'Datum' n.d.; the origins of the concept may be found in Szabo 1997.

[906] Bournez and Ardagna 2011, p.303.

[907] Cf Becker, Malkis and Bussard 2010, p.28.

[908] Kot 2015; D'Acquisto and others (ENISA) 2015, p.44.

[909] D'Acquisto and others (ENISA) 2015, p.44.

[910] Davidson and others 2011, p.9.

[911] Eg The Norwegian Data Protection Authority 2015, p.10.

[912] Eg Yuan and others 2014; in detail, The Norwegian Data Protection Authority 2015, pp.10–18.

conditions. Such data use is logged for the purposes of settlement between the parties taking part in this trade. Therefore, in principle, it could be also available to DPAs or data subjects for accountability.[913]

So, it seems that there is a potential in this area, and businesses, if required to deliver accountability technologies by privacy law,[914] could respond with a framework enabling enforcement of privacy management and accountability of practice. This is because many technologies to achieve this, such as usage control, sticky policies, audit logs, and data tracking are already in place and (sometimes) in use for business purposes. Also, the extent of those technologies shows the possible range of services of PIAs. This is because tracking the use of data and related events are building blocks for their services and the way they are presented to data subjects.[915]

D Conclusions

The main outcome from this chapter is that there are no technological obstacles to implement PMM. On the contrary, most relevant architectural tools have been found and the possibility of the development of additional ones, necessary for PMM, has been confirmed.

More specifically, there are existing technologies to express privacy decisions and communicate them to service providers, like P3P, but they need to be improved to cover all service providers, simplified, and extended to provide data subjects with actual control over data and feedback about results of their actions. Furthermore, it has been shown that the interfaces for the organising function of PMM can be developed. To that end, the technology used by service providers is ready to provide both access to multiple service providers from a one-stop shopping interface, and individual access to more complicated privacy settings and data in privacy dashboards.

---

[913] Cf Betkier ("Individual Privacy Management") 2016, p.329.

[914] As suggested by Bennett 2010, p.8.

[915] See more in the next chapter in Part B s 3 ('Closing gaps in planning').

Also, it has been shown what the core of the organising function of PMM might look like. In this respect, this chapter has proposed the 'ontology' of data and data uses necessary to present data subjects with simple options on a higher level of abstraction. It has also shown how this schema could be presented to the data subject in the user interface of the PIA. This verified that it is possible to achieve a considerably simple design for such an interface.

Finally, it has been found that the enforcement of PMM policies in the ICT systems of service providers and holding them accountable with the help of technology is a promising area. Although technological enforcement is limited, existing practices used to handle personal data in privacy-aware organisations cover much of the desired functionality. To make such systems ready for PMM, they need to recognise standardised types of data and data use and increase data subjects participation in data processing by enabling them to monitor enforcement of privacy policies and, therefore, enabling accountability. It seems that there is potential in this area and businesses, if required to deliver accountability technologies by privacy law, could implement a framework enabling enforcement of privacy management and accountability of practice.

This chapter has shown the technology tools and discussed the way they can implement the market tools presented in the previous chapter. However, as concluded several times, the online industry is not able to implement privacy by itself because of the market problem in which poor quality, privacy-invasive products are driving out better quality ones. This race to the bottom needs to be stopped by appropriate legal tools, described in the following chapter.

VII How to Construct Laws for Privacy Management

The previous chapters have shown which market and technical tools can implement effective privacy management. Now, it is time to define the legal recipe for putting those solutions in place.

To do this, firstly, Part A marks the gaps in current privacy laws in the European law, Australia, Canada, and New Zealand. That is to say, it describes the origin and content of statutory level privacy laws and verifies how they fit into privacy management. In doing so, it looks at so-called Fair Information Practice Principles (FIPPs), which form the operative core of the privacy laws in all researched jurisdictions. The chapter examines early privacy recommendations to check how FIPPs were designed and what problems are inherent within them. It also describes national privacy laws built on the basis of those privacy principles and reflects on their capacity to implement privacy management. Additionally, it formulates some conclusions as to the deficiencies of procedural approach to controlling privacy processes.

Secondly, Part B concentrates on closing the gaps which have just been identified. It describes in detail how privacy management should be applied on top of the most advanced privacy law – the EU General Data Protection Regulation (GDPR). It uses the evaluation criteria of PMM presented in Chapter IV as operational goals. For each goal (ie each functionality of controlling, organising, and planning) it checks the GDPR's ability to achieve it and describes the additional legal measures necessary to do it. This is done in three steps, each of which relate to a core function of privacy management: controlling, organising, and planning.

Part C finishes closing the gaps by describing the legal requirements of a more general character necessary to implement PMM. It presents a way in which implementation of privacy management laws could be supported and secured by enacting an overarching legal principle of informational self-determination. It argues that such a principle containing a substantive, positive liberty needs to replace the FIPPs-based model, and that this is possible in Europe, or perhaps even already being developed there. Furthermore, it shows how privacy management laws should cover services delivered from abroad. Finally, it describes a few smaller, but important problems related to focusing regulation precisely on privacy-invasive activities,

avoiding mixing of PIAs incentives, and avoiding potential problems related to binding up services with blanket consent for data processing.

A Marking the Gaps – Privacy Management in the Laws Based on Fair Information Practice Principles

Data privacy laws across the globe are based on sets of principles which provide a common language for privacy.[916] They all can be traced back to the idea of Fair Information Practice Principles (FIPPs) from the early 1970s,[917] and are collectively called FIPPs in this thesis. This Part explores them to consider how they were developed and applied in privacy laws in the researched jurisdictions, and, most importantly, how they fit into privacy management. To that end, section 1 explores early ideas about privacy laws and the common characteristics of FIPPs. Section 2 looks into contemporary privacy laws in the researched jurisdictions and maps these laws onto privacy management activities. Finally, section 3 formulates some conclusions about the approach of FIPPs which will be important for further discussion.

1. *Why there is little privacy management in national data privacy laws*

The exact composition of a given principle set and its manner of application in the legal order varies depending on jurisdiction. But, in every jurisdiction under analysis here privacy principles create the operative core of data privacy laws.[918] They define the norms relating to processing personal data in general, and, by so doing, also define what the relationship between data subjects and online service providers looks like. So, it is important to examine FIPPs as they also show the current management model for personal data.

---

[916] Gellman 2017, p.38.

[917] Which was expressed fully in Secretary's Advisory Committee on Automated Personal Data Systems 1973, pp.40–41, 59–64. Note that the name 'FIPPs' originates from this document, but is used in this thesis to describe the broader idea of such principles.

[918] They often have a position of legal rights.

To find this model and the ideas which underpin it one needs to examine the early recommendations and proposals of the privacy principles developed in 1970s–1980s. In this respect, particular attention should be paid to three recommendations:

- The British report of a Committee on Privacy, known as the Younger Committee of 1972;[919]
- The US report of the Advisory Committee on Automated Personal Data Systems of 1973;[920]
- The British report of the Committee on Data Protection under the chairmanship of Norman Lindop of 1978.[921]

These reports containing early ideas about privacy protection are compared with two international instruments which form the current framework of reference to privacy statutes in the researched jurisdictions:

- The Council of Europe Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (Convention 108) of 1981;[922]
- The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Guidelines) of 1980.[923]

The juxtaposition of the recommendations and principles from the above documents (collectively 'FIPPs') is attached to the thesis as Schedule A. That comparison aims to find the reasoning behind privacy principles in their current form, and the ideas which led to their development.

The first observation to be made about FIPPs is that they all foresee a balancing of privacy interests with some other interest in the use of data, and, as a result, they all define procedural principles. The conceptualisation of this 'other interest' and its relative strength is different in different documents (eg use of computers for business purposes, or fundamental value of the free flow of information).[924] Similarly, the reasons for balancing are different: need to address

[919] Committee on Privacy, Home Office 1972.

[920] Secretary's Advisory Committee on Automated Personal Data Systems 1973.

[921] Committee on Data Protection 1978.

[922] Adopted in September 1980 (similarly as the OECD Guidelines), but opened for signatures in January 1981.

[923] The OECD guidelines underwent revision in 2013, which put more emphasis on accountability principle.

[924] See row "0" in Schedule A.

problems which are dangerous in public perception,[925] need to regulate the use of data for mutual and shared purposes,[926] safeguarding "everyone's rights and fundamental freedoms … taking account of the … flow … of personal data",[927] or "reconciling fundamental but competing values such as privacy and the free flow of information".[928] The differences in these formulations shift emphases and, therefore, the effects of the balancing exercise. But, the main point is that so-called 'privacy principles' are de facto the rules of balancing. They do not protect the privacy of individuals directly, but by setting rules for the *use* of personal data. They all presuppose that data have to be used and give a framework and limitations for using them. Such limitations take the form of *procedural* safeguards, because they come from the assumption that data are not controlled by individuals. For example, such an approach is clearly seen in documents from works of the US Committee when Miller, co-author of the draft of 'Procedures to protect individuals',[929] presented his ideas about "informational rights of due process".[930] This concept of procedural safeguards appeared to be the most influential idea in the first decade of data privacy which has survived until today in practically every data privacy law.

The second observation about FIPPs is that it is possible to discern among them a few functional groups which address different aspects of data processing: risk minimisation, informing individuals, and individual participation (or controlling).[931] In this respect, starting from the US FIPPs, all sets of the early principles contained provisions to make the individuals

---

[925] Committee on Privacy, Home Office 1972, para.582.

[926] Secretary's Advisory Committee on Automated Personal Data Systems 1973, p.40.

[927] Preamble of Convention 108.

[928] The OECD Guidelines are playing privacy interests down. Eg "...there has been a tendency to broaden the traditional concept of privacy ('the right to be left alone') and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties", the Explanatory Memorandum OECD 1980, para.3.

[929] "Draft Thematic Outline of Report of Secretary's Advisory Committee on Automated Personal Data Systems" of 7 June 1972, Hoofnagle n.d.

[930] "One of the things I have argued for in the few years I have been involved in this problem of privacy is greater legislative awareness of the ability to use statutes to create informational rights of due process, limit data collection, to limit data assembly or aggregation, to enforce codes of professional ethics on data users and data processers, to force, for example, the use of fail-safe or protective devices on information systems, to limit dissemination, to give people rights of access, to compel expungement", ibid., p.268.

[931] In the same way as the thesis presented them in Chapter II.

aware of existence of their personal data and the fact of their processing. While some of the first proposals (ie the US FIPPs and Lindop Committee principles)[932] foresaw making individuals aware of every use of their data, subsequent international instruments (Convention 108 and the OECD Guidelines) either abandon this or shift towards a vague concept of 'openness'. This might have happened due to the perceived impracticality of giving individuals more insight in the era in which there was no Internet access, so data subjects have no possibility of remote access to their data.

Thirdly, in each set of principles there is a common model of controlling personal data described as purpose specification (or use limitation) principle. That is to say, every set of FIPPs contained the rule about individual authorisation to use data outside of the original purpose for their collection (made known at that time).[933] The purpose limitation principle forms the controlling model of FIPPs used until today. It may be traced back to Westin's ideas that consent for information collection is bound up with the purposes for which information is revealed,[934] and, that every further circulation of such information requires additional authorisation by the means of additional consent. This was described as a two-step model of 'legal control of the dossier' by Goldstein.[935] In his view, such a model is a practical way of effecting control by the means of consent and waiver given in the initial communication to the other party. The role of waiver is to waive individual's rights over the data for use for specified purposes. Using data for any other purpose not included in the waiver requires subsequent consent. Despite the purpose limitation, consent was not yet perceived as necessary for the initial collection of data. Individuals had rights to access data,[936] but such access was envisaged to keep data correct rather than to allow individuals to decide about data processing.[937] This absence of initial consent may be explained by the fact that in those times

[932] The Lindop Committee proposed providing individuals with full information about data and their uses.

[933] Note that the rules of the OECD Guidelines related to re-use of data outside the original purpose are more relaxed.

[934] Westin 1967, p.375.

[935] Goldstein 1969.

[936] Such rights were also in the first data privacy law on the national level in Sweden (1973), Secretary's Advisory Committee on Automated Personal Data Systems 1973, p.170; cf also with 'the right to printout', Committee on Privacy, Home Office 1972, p.618.

[937] Mayer-Schönberger 1997, p.224; also, Kosta notes that the focus of the OECD Seminar in 1974 was on rights of access, rather than rights to decide about processing, Kosta 2013, p.29.

data were collected mainly in paper form. Submitting such a form was equal to consenting (unless, of course, that was obligatory), so additional authorisation was not practical or necessary.

Initial, separate consent for data processing appeared slightly later and was related mainly to European law. It was the German Federal Data Protection Act of 1977 which put individuals in a position to decide about data processing by establishing consent as one of two possible legal bases for data processing (along with other statutory provisions).[938] This Act also made clear that it did not protect personal data per se, but protected the privacy of individuals by protecting their data from misuse.[939] This was a turning point, which together with the technological shift from mainframe supercomputers to a more decentralised environment of data processing by microcomputers, shifted discussion in Europe towards individual privacy rights.[940] This transformation culminated with the recognition by the BVerfG in 1983 of the right to informational self-determination[941] which further extended the boundaries of Westin's definition of privacy. As the German data protection rights were very influential in Europe, some of the German concepts were replicated at the level of the European Union.[942] However, parallel to the development of individual rights in Europe, there was another factor which gained major importance in the regulation of data privacy as early as the 1970s: importance of personal data for business in an increasingly interconnected world.

The use of data for business purposes slowed down or even stopped the development of privacy rights. The lack of harmonisation of data privacy laws started to be a serious trade issue in the mid-1970s.[943] Discussion about balancing privacy protection with business needs was conducted by two institutions: The Council of Europe (CoE) and the Organisation for Economic Co-operation and Development (OECD). While in 1970s and 1980s the former

[938] Section 3 of the Act, translation in Kosta 2013, p.50; for detailed description of the Act, see Riccardi 1983.

[939] Riccardi 1983, p.248.

[940] Mayer-Schönberger 1997, p.226; private enforcement was considered as an American model; see the discussion in Committee on Data Protection 1978, para.4.27.

[941] This term was first used in Mallmann 1976, pp.47–80; description of early German research in the area of data protection, Burkert 2000, p.49.

[942] The best example is the name 'data protection' which is a calque from 'Datenschutz'.

[943] Eg in 1974 the Swedish Data Inspection Board banned the export of personal data to the UK because of the lack of regulations there, Burkert 2000, p.51; Warren and Dearnley 2005, p.244.

contained mainly Western European countries, the latter included others: the United States, Canada, Australia, and New Zealand.[944] The OECD was, therefore, the first main forum for exchanges between North America and Europe on privacy legislation, with, as reported, Asian and Pacific countries participating more as observers.[945] There was a need for a broader compromise taking into account the differences in legal cultures.[946]

There are clear differences in the approaches of the two international instruments prepared by these organisations. While Convention 108 puts some emphasis on the need to safeguard human rights, the OECD Guidelines' goals are shifted more towards enabling the use of data. For example, in the Guidelines, the aspect of data controlling (named 'individual participation principle') includes: the right to know about data collection, the right to access to data, and the right to "challenge data". In Convention 108 controlling contains additionally a right to rectification or erasure, and a right to remedy. Although the CoE instrument might have broader impact since it was adopted by more countries[947] and, once ratified, it required member states to adapt their laws,[948] the Guidelines had more impact in the researched jurisdictions outside the Europe.[949]

Notwithstanding these differences,[950] the Guidelines and Convention 108 do little to effect privacy management. Their principles are slightly different and Convention 108 gives slightly more control over data, but, nevertheless, the substantive scope for individual action in either of them is narrow. As a result, national privacy laws which transpose those instruments also give little scope for privacy management.

The creation of these two instruments was also a moment where data privacy laws from the considered jurisdictions went in clearly divergent directions. Canada, Australia, and New Zealand implemented in their early statutes OECD Guidelines (respectively in 1983, 1988,

---

[944] Australia became a full member in 1971 and New Zealand in 1973.

[945] Burkert 2000, p.51; Kosta 2013, p.27.

[946] Kirby 2016.

[947] 50 countries including three non-members of the CoE (as of 9/6/2017).

[948] See Article 4. However, there are no 'strengthened' enforcement mechanisms (like the jurisdiction of the ECtHR).

[949] A thorough description of world privacy laws, Greenleaf 2014.

[950] Also, Convention 108 covers only "automated data files and automatic processing of personal data".

and 1993).[951] The UK, as a member of the UE, followed the course of European law, and, European law was further harmonised within the European Union. It is time to describe how FIPPs were implemented in data privacy laws in these jurisdictions.

2. *How the contemporary national data privacy laws fit into privacy management*

So how do national data privacy laws fit into the search for the elements necessary to implement privacy management? The relevant statutory instruments from the researched jurisdictions are juxtaposed in Schedule B,[952] and broken down into the same categories which were used in the previous section. As can be observed there, there are differences between countries in the implementation of FIPPs. There are, also, additional elements of controlling specific to European law (eg right to erasure).[953] This reflects the split in the privacy laws mentioned in previous section, ie the European law took a separate path with a more prescriptive approach, while the remaining researched countries followed the OECD Guidelines. The reason for the further harmonisation in the EU was the lack of adoption of Convention 108 by some of its Member States,[954] and differences in those national laws which adopted the Convention.[955] The response for this was the Data Protection Directive (DPD) enacted in 1995.

Besides harmonising the laws, the DPD aimed to strengthen protection of fundamental rights. To that end, it developed the Convention's 108 flexible 'additional safeguards' (principles) into stronger legal requirements. For example, there are legally enforceable rights of access to

---

[951] In the case of Canada and Australia those Acts covered only public sectors. Australia extended protection to part of the private sector in 2000, and Canada enacted PIPEDA (regulating private sector) in the same year.

[952] The UK Data Privacy Act 1998 is not listed there because it would mainly repeat European DPD. Nevertheless, the peculiarities of the British application of DPD are indicated in the text where appropriate. Also, the European ePrivacy Directive is not listed but mentioned in the text below.

[953] Rows 14-17 in Schedule B.

[954] Italy, Greece, Belgium, and Netherlands. This caused problems with data transfers, such as the intervention of French DPA (CNIL) stopping data transfer to Italy (Fiat case). Bennett and Raab 2006, p.53.

[955] Bennett and Raab 2006, p.53; Kosta 2013, pp.84–85.

data (Article 12),[956] to object to the processing (Article 14), and not to be the subject of purely automated decisions (Article 15). A more rigid approach may also be seen in specifying the general prohibition of data processing and limiting the legal basis for lifting this prohibition (in Article 7), or in formal conditions to the data subjects' consent.[957] Consent in the DPD is interesting from the point of view of controlling function of privacy management. It is one of six possible legal grounds for data processing (Article 7(a)),[958] and one of the legal grounds for processing of sensitive data (Article 8(2)(a)). It may be argued that it is the main ground for service providers, because only processing based on consent is not restricted to 'necessary' activities and may justify processing of more extensive set of data.[959] Also, consent is used to overcome the purpose limitation, and as one of the derogations from prohibition of transfer data to the country without adequate level of protection. Furthermore, according to the implementation of the DPD in some Member States, data subjects' consent could be withdrawn or revoked, but with no retrospective effect.[960] Similarly, in some cases in which processing is not based on consent[961] data subjects have the right to object (Article 14), so the right to challenge data processing activities of the controller and stop that processing.[962] These

[956] However, according to the CJEU the sole purpose of the right of access is to allow the individual to check lawfulness and correctness of one's data, so demands to access for other purposes, eg to 'obtain access to administrative documents' may be rejected, Case C-141/12 *YS* [2014] CJEU, paras44–46.

[957] Ie freely given specific and informed indication of one's wishes (Article 2(h)), which need to be additionally explicit (Article 8(2)(a)), or be given unambiguously (Article 7(a)).

[958] Interestingly, in the first proposition of Directive consent was the only ground for lawfulness of data processing in the private sector with just three exceptions to this, proposal of Article 8, European Commission 1990, pp.24–25; this approach was, however, criticised and rejected in the first reading of the European Parliament, Kosta 2013, pp.95–96; nevertheless, seven Member States put consent as the only (or, in fact, main) basis for processing (with exceptions) in their transpositions of the DPD, Korff (ETD/2001/B5-3001/A/49) 2002, p.73.

[959] There are two other options under Article 7 for a service provider: processing necessary for performance of a contract (b), and processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (f). The last one, although at first glance it may seem appealingly broad, is limited in many countries, should be carefully balanced with interests of data subjects and, according to the opinion of Article 29 WP, should not be treated as a 'last resort'. See Article 29 WP (WP 217) 2014; Carey 2015, pp.87–88.

[960] Korff (ETD/2001/B5-3001/A/49) 2002; Kosta 2013, pp.251–254.

[961] But, on the grounds of 'legitimate interest', or 'public functions'.

[962] Successfully claimed in Case C-131/12 *Google Spain* [2014] CJEU as the 'right to be forgotten'.

are all elements of the controlling function of PMM related to accessing information and making decisions by data subjects.

However, from the perspective of the PMM implementation, there are practically no elements of organising or planning in DPD.[963] But, some elements of organising on top of controlling elements can be found in ePrivacy Directive which applies to the processing of personal data in the electronic communications sector. Individual control over data has been applied there even more broadly than in the DPD. For example, its provision of Article 5(3) contains a right to refuse for storing information and gaining access to information stored on the terminal equipment of the user (known commonly as a 'cookie law').[964] The 'right to refuse' is nothing different from consent, even though it is applied in a specific way.[965] Furthermore, consent is explicitly and very often used in the ePrivacy Directive. For example, consent is a *necessary* ground for processing of some types of data: traffic data (Article 6) and location data (Article 9). These two uses of consent also show an aspect of organising, because decisions of individuals apply to standardised types of data (traffic, location). Similarly, an aspect of organising may be found in specifying particular uses of data in Article 12 (consent for including individuals' names in a public directory) and Article 13 (consent to receive marketing communications).[966] Organising is related to having data prepared for management and discerning those categories allow individuals to make decisions as to their use (eg give or revoke consent for use of traffic data). These examples are useful, because they show that narrow elements of privacy management are already in law.

Both directives, the DPD and ePrivacy Directive, give some flexibility with the means for expressing consent in electronic form. DPD applies a purely functional approach – it specifies that consent should be always 'freely given', 'specific', and 'informed' (see Article 2(h)), sometimes 'unambiguous' (see Articles 7(a), 26(1)(a)), and sometimes explicit (Article 8(2)(a)), but it does not give any prescriptions as to the form. Interestingly, on the level of the

[963] Distinguishing special categories of data in Article 8 is hardly an organising factor.

[964] As ePrivacy Directive applies to communications services, it uses terms 'subscriber' or 'user'.

[965] However, some authors say that opt-out choice is not a consent, Kosta 2013, p.202.

[966] Also, the German transposition of DPD distinguishes between processing "for one's own purpose" and "for the purpose of disclosing data", and lays down differing criteria for each, Korff (ETD/2001/B5-3001/A/49) 2002, p.74.

national law, Germany gives additional flexibility by explicitly specifying adequate forms,[967] while the UK achieves the same goal by not defining consent at all.[968] This flexibility allows service providers to implement consent in electronic form (eg with tick-boxes).[969] Furthermore, the preferred way of implementing the right to refuse for storing information (eg 'cookies') on terminal equipment is expressing the choice in the interface of Internet browser. This is also an element of the organising function of PMM, which requires technical interfaces to express choices related to data collection and use. So, these examples indicate that the use of technical interfaces for privacy management is nothing unusual in law.

The trend to increase the participatory role of data subjects in data processing was sustained in the latest legislation, the General Data Protection Regulation (GDPR), which has applied since 25 May 2018.[970] European regulations are directly applicable in all Member States,[971] so the new law will be binding in its entirety and will substitute any national laws in the scope of its application.[972] As shown in Schedule B, the GDPR further extends rights to access and to object, narrows down conditions for valid consent and explicitly enables its withdrawal. Furthermore, the GDPR introduces new rights to restriction of processing, to erasure (extending the 'right to be forgotten' as defined by the CJEU) and to data portability. This creates a completely new generation of privacy laws. Importantly, the enforcement of those rights may be enhanced because of the high fines for non-compliance, and new rules for judicial remedies simplified for data subjects (ie jurisdiction of the local court and possibility of being represented by a non-profit body association).[973] In comparison to other researched jurisdictions, this gives more space for individual participation in data processing. So, the GDPR is a development towards privacy management, but it still lacks many important features of the entire privacy management system. The details of its deficiencies in this respect are discussed in the next Part.

---

[967] Korff (ETD/2001/B5-3001/A/49) 2002, p.74.

[968] Ibid., p.27.

[969] ePrivacy Directive, recital 17.

[970] See also, a proposal for new e-Privacy Regulation is currently being discussed, European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[971] In opposition to the EU directives, Article 288 of the TFEU. The GDPR has applied also in the UK regardless of the 'Brexit' process.

[972] As 'stemming from the Treaty', eg Case C-11/70 *Internationale Handelsgesellschaft* [1970] CJEU, para.3.

[973] Articles 79 and 80.

In contrast to Europe, Australia, Canada, and New Zealand took a different tack, related more to their common law traditions[974] and the standard introduced by the OECD Guidelines. Australia and New Zealand adopted an approach in which organisations processing personal data[975] have to comply with a set of high-level flexible principles. Those are, as a rule, not directly enforceable in a court of law,[976] and may be shaped according to particular circumstances by the companies applying them and by DPAs. The third common law country, Canada, took a slightly different approach of adapting as a standard the Canadian Standards Association (CSA) Model Code.[977] This standard, also based on FIPPs, was worked out in a multi-stakeholder forum in 1990s.[978] As a result, the Canadian privacy principles put more emphasis on consent, probably even more than the DPD. This is because consent is a prominent, separate principle required for data processing. In so doing, however, they leave much flexibility regarding the form of consent and the way it may be given. For example, they allow service providers to use an opt-out schema or even to imply consent where individuals may have a reasonable expectation that their personal data would be used in other ways.[979] This seems to be a much more pragmatic and powerful approach than in Europe, however, it gives preference to societal standards (by the means of an objective expectation of privacy) rather than to individual, subjective perspectives.

The preference given to objective standards of privacy over individual privacy management is a salient characteristic of these three countries. It is even more prominent in Australia and New Zealand, where individual participation in data processing is on a low level. For example, there is no specific consent requirement for data collection, which means that data may be

---

[974] Because they do not create the abundance of privacy-related rights, see below.

[975] However, in Australia only those private sector operators, which are not classified as small business, so having more than AU$3m of turnover, Privacy Act 1988 (Cth), ss 6C and 6D.

[976] With the exception of the New Zealand 'Access principle', Privacy Act 1993, s 11; see also injunctions in Privacy Act 1988 (Cth), s 98.

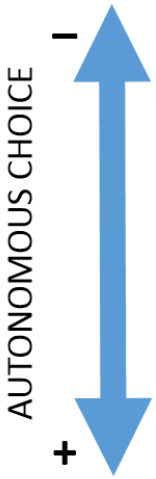
[977] Ie CAN/CSA-Q830-96, PIPEDA, sch 1.

[978] McNairn 2007, pp.1–3.

[979] In particular PIPEDA, ss 4.3.3 - 4.3.7 sch 1. Such an approach in some European states (eg Germany) would not be considered consent because of the lack of a clear signal about intentions. However, the Canadian approach is similar to the approach in the UK and Finland, European Commission 2003, p.5.

collected without individual authorisation at all. [980] Or, as usually happens with regard to online services provision, consent may be concatenated to the acceptance given when entering into contract. Also, the purpose limitation principle which is the common model of control over data has more exceptions in Australia, Canada and New Zealand. Furthermore, a common characteristic of Australia, Canada, and New Zealand is that the enforcement of data privacy laws is relatively weak. In the case of a dispute, there is an emphasis on reaching a settlement during the proceedings before DPA, with judicial oversight in cases where parties are not willing to agree and settle. A low level of individual participation and weak individual enforcement makes these laws less suited for privacy management.

To present how laws in all researched jurisdictions fit privacy management, their normative elements were juxtaposed with the non-normative elements providing data subjects with varying levels of autonomous choice in Figure 24 below.



Non-normative	Normative elements in data privacy laws	
Minimising risks, excluding data, securing storage and access	Obligation to secure data, data minimisation principle	Right to fair and lawful processing (procedural) Accountability
Knowing about collection and use	Obligation to provide information about collection and use	
Consenting to collection and use	Obligation to obtain consent to a given purpose/use	
Controlling the process of data collection and use	Right to access, correction, withdraw consent	
	Right to object, restriction of processing, erasure, data portability	
Managing the process of data collection and use (requires controlling, organising, and planning)	(Right to individual self-determination)*	

* - not an element of data privacy laws in the researched jurisdictions

Figure 24 Non-normative and normative dimensions of privacy in the national data privacy laws

This figure shows that some legal elements of PMM are present in national privacy laws, but they are mainly related to controlling. Firstly, as shown in Figure 24, there is a group of general rules, which organise the process, set accountability, and lower the risks of keeping personal data. Secondly, the rules related to provision of information enable any kind of interaction

[980] But, consent is required for collection and use of sensitive data in Australia, Principle 3, Privacy Act 1988 (Cth), sch 1. Also, there are proposals to implement consent into data privacy law in New Zealand, see New Zealand Data Futures Forum n.d, p.65 ff.

with service providers from the data subjects, because they make them aware of data processing.[981] They are a prerequisite for any exercise of autonomy. They are usually related to initial information provided to a data subject about the scope and purposes of data processing ('notice') and applicable procedures or rights. This standard seems to extend to cover notification about data breach. Thirdly, rules related to consent with all their limitations and in varying degrees, as discussed above, give individuals some autonomy as to the collection and use of personal data. Fourthly, there are some additional elements of controlling the process. All jurisdictions foresee access rights, and abilities to correct data. This is not much, though, and it does not enable effective controlling. For example, withdrawing consent is not provided for in Australia in New Zealand. Furthermore, only the European laws have additional controlling elements, such as rights to erasure ('the right to be forgotten'), restriction of processing, and data portability.[982] However, all these elements pertain mainly to the controlling function of privacy management. Also, there is currently no right at the constitutional level[983] which could underpin the entitlements to all privacy management activities. This aspect will be discussed thoroughly in Part C.

To sum up, national privacy laws facilitate some elements of controlling function of privacy management but, as they give very little organising and planning, they do not provide for PMM. The European laws provide more legal tools for controlling data by individuals and stronger enforcement, but they are imperfect. What is the value of the most rigorous consent procedure if the definition of the scope of such consent is vague and can be changed any time by service providers? How can data subjects determine who knows what about them if they cannot set goals for the future nor reflect about the past use of their data? At the same time, Australia, Canada, and New Zealand put more emphasis on objective, societal standards of privacy and individual control is not well developed there. In general, all these laws are procedural in nature and have not developed a substantive, normative entitlement to privacy management. What are the drawbacks of a procedural approach?

---

[981] However, it is questionable that they give much knowledge about what is happening with the data.

[982] There is also quite peculiar provision related to automated decision making, which seems to address only a very narrow aspect of use of personal data, Bygrave 2001, p.17 ff.

[983] The rights are considered as constitutional when they have a higher status in a legal system. Note that they do not have to be included in a written constitution. Rivers 2010, p.xix.

3. *The deficiencies of a procedural approach*

All the laws just discussed are based on the concept of FIPPs. They try to involve individuals in the data process of businesses to a different extent, but the outcome, as described in detail in Chapter III, is consistently unsatisfactory. People overwhelmingly signal that they lose control over their personal data and do not feel comfortable about it.[984] None of the legal approaches discussed above have provided any viable solution to this so far, which leads to the point that FIPPs may be simply outdated and no longer fit for purpose.

FIPPs, indeed, received a lot of critique related to their obsolescence. As noted above, they are the result of a balancing exercise between privacy and some other value (differently defined in many instances of FIPPs formulation). Such balancing involves defining two contradictory values or principles[985] with the permissible level of detriment to one of them depending on the importance of satisfying another.[986] But that balancing was done 35–45 years ago where the privacy 'threat model' was related to a small number of 'data banks' processing data in a predefined sequence in isolation from individuals.[987] It was possible then for individuals to know where their data were and what their scope was because the fact that communicating data to the data bank was usually related to responding to an inquiry or filling out some paper form. Yet, in 1996 Laudon claimed that contemporary large-scale databases operated by PC-based networks made it impossible for individuals to know where their data were.[988] Now, roughly 20 years later, the network is much faster and online services are able to perform real-time tracking (often without the data subject's knowledge), collection, processing, and dissemination of personal data. Therefore, the level of encroachment into privacy of individuals has increased dramatically. Similarly, the way the privacy interests of individuals are conceptualised has changed. So, it may be argued that a new balance has to be

---

[984] Eg Information Commissioner's Office 2015, pp.4–5; Kleiner Perkins Caufield Byers 2016, p.209; TNS Opinion & Social (DS-02-15-415-EN-N) 2015, pp.9–14.

[985] Values represent what is 'good', while principles represent what 'ought to be', von Wright 1963, pp.6–7.

[986] Eg Alexy 2010, p.102.

[987] Albers 2014, p.229.

[988] Laudon 1996, p.96.

found which takes into account the contemporary context,[989] and/or substantive rules should be introduced to describe the interests of individuals.[990]

Just as the legal procedures of data privacy were designed in a completely different technological reality, they set goals which neither safeguard individuals from modern technology, nor reflect current privacy values. The problem is that compliance with those partial but specific rules becomes the singular end,[991] which may be specifically well observed in European law, where the procedure of consent gained recognition at the constitutional level.[992] So, the goal of protecting the individual has been substituted by serving appropriate notice (or disclosure) and collecting consent in a legally specified form. As a result, individuals often receive an 'onslaught' of notices with (usually) limited choice.[993] Such an approach is mechanical, formal, and reduces the privacy regime to purely legalistic and procedural order.[994] At the same time, as observed by Marx, those procedures are "insensitive to the question of violations and trust",[995] because the formal requirements relieve service providers from legal risks. As many authors underline, there is little or illusory control over data collection and use.[996] As a result, the risks for data subjects are removed neither by the service providers nor by data subjects themselves.

Furthermore, such procedural rules have eroded in favour of convenience with corresponding reduction in concerns about the risks and underpinning privacy values. For example, the purpose (or use) limitation principle in national data privacy laws gets more and more exceptions.[997] Those exceptions increase the flexibility of privacy rules but also decrease the

---

[989] Bonner and Chiasson 2005, p.286.

[990] More in Part C.

[991] Bamberger and Mulligan 2015, p.34.

[992] ChFREU, Article 8. Cf with Hustinx, who is of the opinion that this recognition does not change the status of consent as being merely one example for legitimate basis for personal data processing, Hustinx 2013, p.22. This, however, seems to be hard to reconcile with the assumption about rationality of the legislator; similarly, Rouvroy and Poullet 2009, p.72.

[993] Cate 2007, p.341.

[994] Eg Gilliom 2011, p.503; Cate 2007, p.341.

[995] Bennett 2011, p.492.

[996] Eg Laudon 1996, p.97; Diaz, Tene and Gürses 2013, p.929.

[997] Schedule B row 11.

level of protection.[998] It seems that the initial idea of the controlling model of FIPPs described in section 1 as a combination of consent and waiver[999] is no longer able to deliver control over the process of data collection and use. The problem with overcoming this problem is that the perspective of legislators is dictated by the existing FIPPs model and they still look for improvements *within* this model. This was clearly seen in the process of revision of the DPD (leading to enacting of the GDPR), in which the European Commission, after clearly and correctly posing the problem as "difficulties for individuals to stay in control of their personal data", addressed this with the statement about improper transposition of DPD into the national laws and lack of awareness of individuals.[1000] Such a response does not tackle the problem, or at least there is no indication that it does so, but keeps reapplying the FIPPs model by providing data subjects with more information and strengthening consent requirements. Instead of enacting 'FIPPs+' (eg the GDPR), the focus should be moved back from procedural principles towards more substantive approach. Such a substantive approach is presented in the next two Parts: in Part B by showing how to implement privacy management activities (controlling, organising, planning), and in Part C by showing a substantive principle underpinning those activities.

B Closing the Legal Gaps – Privacy Management on Top of the General Data Protection Regulation

So, what exactly needs to be improved? The best way to show it is by presenting the gaps between the General Data Protection Regulation (GDPR) and the Privacy Management Model (PMM). The GDPR has been chosen for this task because, as discussed above, it is the most advanced in the development of privacy management. Furthermore, as shown in Chapter IV, EU law is the best place to implement PMM because it exports higher privacy standards to other jurisdictions. Having said that, it has to be kept in mind that the GDPR is a regulation based on a procedural approach, so, as just discussed, PMM should not be simply added to the GDPR. Instead, the PMM implementation would need to change many GDPR elements (most notably the consent requirements) as indicated in this Part, and should come together with a

[998] Eg 'directly related purpose', Privacy Act 1993, s 6, Principle 10(e); GDPR, Article 6(4).

[999] As described by Goldstein 1969.

[1000] European Commission (SEC(2012) 72 final) 2012, p.21.

substantive legal principle underpinning privacy management (which is described in the following Part C).

So, the differences between the GDPR and PMM have the most relevance for practical application of this thesis. These differences are presented in three consecutive sections related to controlling, organising and planning. They identify the gaps in each of these functions and show how these gaps can be closed. The goal is set on the basis of evaluation criteria described in Chapter IV and also presented below:[1001]

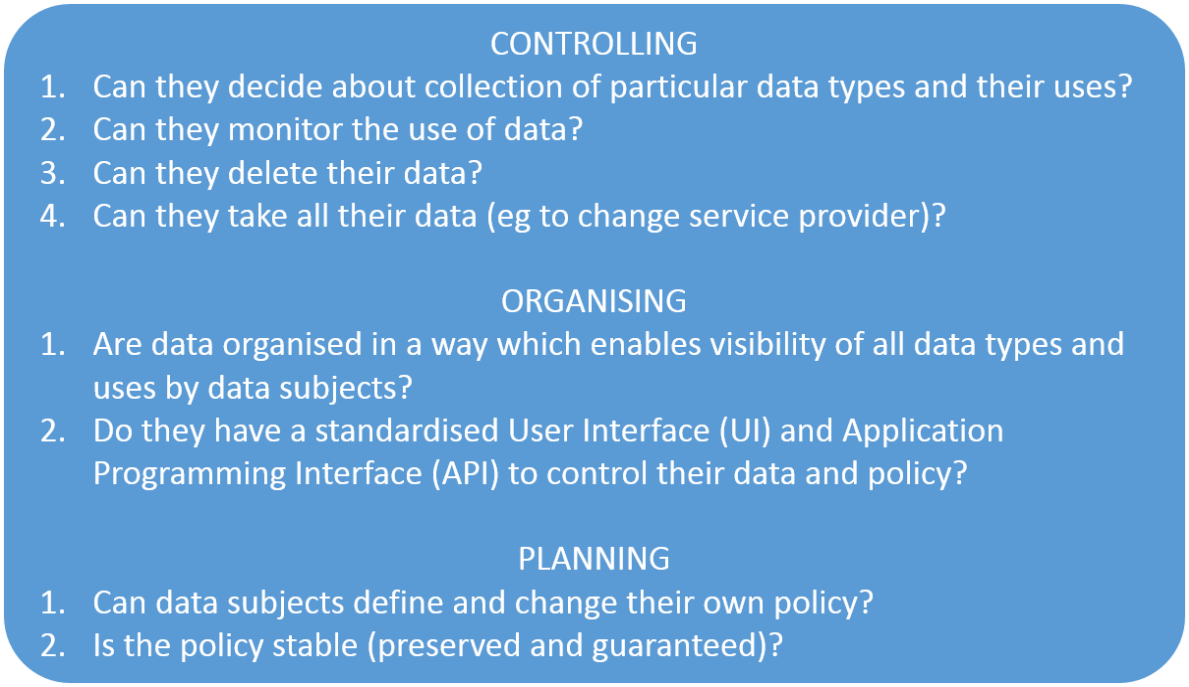


Figure 25 Evaluation criteria for data subjects' autonomy in PMM

1. *Closing gaps in controlling*

As described on a general level in the previous Part, the controlling function is already present in the GDPR, but overly focused on consent. A general impression is that the GDPR is very complicated in this respect. There are many separate rights – to access, to object, to restrict processing, to erasure. Many of these individual rights have restricted use for particular cases

[1001] The order of presenting those criteria is set to show first the differences in areas covered by the GDPR (ie controlling).

depending on the legal bases for processing, or even on particular data purposes. This could be simplified.

(a) Data subjects should be able to decide about the collection of particular data types and their uses

At first glance, the GDPR seems to put a lot of emphasis on informed consent. In so doing, it harmonises the European standard of active consent which cannot rely on silence, pre-ticked boxes or inactivity,[1002] but also does not need to be in writing.[1003] Moreover, Article 7 introduces rules that are supposed to make consent more voluntary and intentional. That is to say, consent should be at least distinguishable from other matters,[1004] possible to withdraw at any time, [1005] and not bound up with collection of data not necessary to perform a contract.[1006] Furthermore, there is emphasis on providing data subjects with abundant information when the personal data are obtained, either directly (Article 13) or indirectly (Article 14), so after consent is given.[1007] The idea seems to be to provide data subjects with a comprehensive, transparent, and easy to understand (Article 12) standard set of information covering inter alia: who processes their data, in which categories, for what purposes, on what legal grounds, for how long they are kept, who may receive those data, together with the information about particular rights which may be exercised by data subjects. This includes some additional explanatory elements such as "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" which need to be provided at least in the case of automated decision making (including profiling).[1008]

[1002] GDPR, recital 32. This introduces change for countries which (like the UK) relied also on other, inactive forms of consent. Note that for processing sensitive data, consent needs to be additionally 'explicit' (Article 9(2)(a)).

[1003] Which is required in some national laws, Korff (ETD/2001/B5-3001/A/49) 2002, p.74. Also, Article 6(1)(a) does not have the word 'unambiguously' which was in DPD. This may decrease the strictness of implementations in some countries, eg Poland.

[1004] GDPR, Article 7(2). This idea seems to be imported from German so-called "linkage-prohibition" (Koppelungsverbot), Korff 2010, p.17; also, Kosta 2013, p.155.

[1005] GDPR, Article 7(3) and recital 42.

[1006] GDPR, Article 7(4) and recital 43.

[1007] Unless there were other legal grounds for data collection.

[1008] GDPR, Articles 13(2)(f) and 14(2)(g).

This seems to be a huge amount of information, which may be, however, provided "in combination with standardised icons".[1009] Looking at the broadness of those provisions it seems very likely that the information will remain unread.

These requirements for consent are even more stringent than in the DPD, but may, in fact, turn out to be counterproductive for the reasons described in Chapter II (eg lack of capacity to understand, lack of meaningful choice). Also, some businesses may be looking for an escape into the 'legitimate interest' category[1010] which may be seen by service providers as a less burdensome opt-out scheme (which, however, does not exist for 'sensitive' data), but is at the same time much more risky.[1011] As the scope of this category is in practice defined by DPAs, this would be a move towards an objective expectation of privacy, therefore in a similar direction as Australia, Canada, and New Zealand, but by slightly different means. This may be beneficial for many businesses which do not engage in activities which may breach informational autonomy,[1012] but may be detrimental to data subjects in the case of many service providers who do so. This is because they will be forced to rely on the general standard of online privacy, which is rather poor.[1013]

Instead of further strengthening consent and information requirements, a better way to empower individuals to decide about their privacy is to enable a separate path of authorisation of data processing by the means of Personal Information Administrators (PIAs) and individual privacy policies in the way described in Chapter V. This path would be obligatory for activities considered risky for individuals, and voluntary for other businesses. This sort of authorisation requires less information provided in disclosure. There is no point in providing burdensome information and consent requests when data subjects have constant access and monitoring of their data through PIA services. Also, it makes little sense to present several screens of privacy policy and check a number of tick-boxes if individual privacy policy stored and secured at PIAs has precedence over T&Cs. It could also lower the costs of consent procedures and their

[1009] GDPR, Article 12(7).

[1010] DPD, Article 7(f); GDPR, Article 6(1)(f).

[1011] Because it requires a balancing test which may be questioned by the DPA, Article 29 WP (WP 217) 2014.

[1012] See Chapter III. Also Part C.

[1013] See Chapter III.

maintenance due to centralisation.[1014] Furthermore, this solution, as discussed in Chapter IV, would be open to many other applications. For example, privacy settings in browsers, mobile apps, or smartphones could be derived from users' settings on a PIA's server. In this way, data subjects would be independent in their privacy actions from all vertically integrated service providers providing their architectural elements (eg Google Chrome), described as a problem in Chapter III. This also has the potential to expand into other applications, like the Internet of Things. In sum, relieving individuals and service providers from consent requirements without leaving them vulnerable to privacy breaches has huge value, as indicated in Chapter IV.

Additionally, as discussed in Chapter V, data subjects should be secured from third-party tracking. Without this, personal data would 'leak' to 'voyeurs' tracking every digital move of the data subjects, which would undermine individual decision making. In this respect, it is worth taking a look at the European Commission's project of the new ePrivacy Regulation[1015] of January 2017. It proposes that the only collection of data from end-users' terminal equipment permitted without explicit consent would be the collection necessary for signal transmission, for the provision of a service requested by the data subject (called there 'end-user'), and web audience measuring performed by the requested service itself.[1016] The Commission also proposes imposing obligations on software providers, to require them to secure individuals from third-party data collection.[1017] These provisions are a very good base to achieve the goal described in Chapter V without breaching informational autonomy.[1018]

[1014] Cf the anticipated savings of €950m on centralisation and automation of consent in the browser software discussed in s 3.4, European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017, pp.7–8, this proposal aims to achieve similar effect, but on a larger scale.

[1015] European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[1016] Article 8(1) and recitals 20 and 21, European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[1017] Article 10, European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[1018] They additionally need to be improved in regard to the prohibition of tracking of the emitted signals, Article 29 WP (WP 247) 2017, pp.11–12; also, European Data Protection Supervisor 2017, pp.19–21.

(b) Data subjects should be able to delete their data

The ability to delete data and withdraw them in this way from further processing is one of the main ways in which data subjects may exercise their informational autonomy. The controlling aspect of the GDPR in respect of this ability seems to be well developed. It comprises the rights to object, to restrict processing, and, finally, the right to erasure ('the right to be forgotten'). The Regulation contains a few separate instances of the right to object, from which the strongest is the right to object to processing for the purposes of direct marketing. This is an absolute right, because when a data subject objects to the processing of personal data, they shall no longer be processed for such purposes.[1019] The same right is not absolute where the processing is based on necessity of action in the public interest or official authority, or on grounds of legitimate interests of a controller or a third party.[1020] In such a case, the controller may continue processing if it is able to demonstrate "compelling legitimate grounds".[1021] The new right to restriction of processing allows individuals to demand such a restriction in situations where the data are contested (including the execution of the right to object).[1022] Finally, the right to erasure is a codified, enhanced and slightly extended version of what was known as 'the right to be forgotten', as in the result of the *Google Spain* case.[1023] The goal is clearly to erase personal data where they are no longer necessary or the base for their processing is not valid (or no longer valid).

This all should be rather effective and there is no sense in adding much to this to achieve privacy management, but it seems that it could be simplified. It seems that the rights to object and to erasure could be drawn slightly more broadly (eg to include data where they are processed on the basis of 'contract performance'). Perhaps even the right to object could be simply an instance of the right to erasure,[1024] so they could form together the right to erase those data which are not relevant for any other prevailing reason. In the case of the existence of such a prevailing reason, service providers after receiving a request to delete data should be

[1019] GDPR, Article 21(3).

[1020] So, GDPR, Articles 6(1)(e) or 6(1)(f).

[1021] GDPR, Article 21(1).

[1022] GDPR, Article 18.

[1023] GDPR, Article 17. Cf Case C-131/12 *Google Spain* [2014] CJEU.

[1024] Processing includes storage (Article 4(2)).

obliged to restrict any commercial activities in relation to those data and erase them immediately after the time of necessary retention (if such a term is determined).

(c) Data subjects should be able to change service provider and take all their data with them

Data portability was discussed in Chapter V as an important concept which could increase competition in the market and unlock new markets re-using personal data for the benefits of data subjects. PMM supported by the legal right to informational self-determination[1025] should enable handing data back to data subjects and ensure effective control over the reuse of those data by other firms. Customers may also be reasonably secured by the PIAs from different, changeable T&Cs of different service providers and the asymmetry of the information.

Furthermore, the right enabling data portability is already provided by the GDPR.[1026] It is applicable only where processing is automated and based on consent or contract and consists of two main elements. The first is similar to the right of access and enables individuals to receive their data, however, in "a structured, commonly used and machine-readable format".[1027] The second element is the right to transmit those data from one controller to another, which may be done, when technically feasible, directly between those controllers. However, data portability is limited to data provided by the data subject, so data which are derived or inferred based on analysis of personal data (and are also personal) are excluded from its scope.[1028]

It may be suggested that the scope of this right should be broader and not based on the way data were collected. All personal data should be available for data subjects to take unless there are prevailing interests in their protection from the data subject.[1029] So, data portability should be applied also to data received from third parties. Such a rule could also remove the risk that

[1025] See Part C.

[1026] GDPR, Article 20.

[1027] GDPR, Article 20.

[1028] Article 29 WP (WP 242 rev01) 2017, pp.9–11; cf voices that 'observed data' may not be in the scope, Meyer 25 April 2017.

[1029] Cf even broader idea, Australian Government, Productivity Commission (No. 82) 2017, p.16.

raw ‘observed data’ could be excluded from the right of data portability because they were transformed into another form (eg saved into a database so that they can now be called ‘derived data’). Having said that, it seems that data which are the product of the algorithms performing personalisation or profiling should not be in the scope of the right to data portability, as they may possibly reveal trade secrets related to these processes. But, all personal data that do not bring any intellectual property or trade secrets of service providers should be available for data subjects.

Another potential problem with the implementation of data portability in the GDPR is the lack of standards to receive and transmit data to new providers. Also, vague “encouragements to cooperation between industry stakeholders” issued by Article 29 WP[1030] show that this part of data portability is still an open book for the future. In this respect, PIAs as main points of contact of different service providers could play a greater role in implementation. This is because they would already have interfaces to service providers and one-off transfers of customer data would be just an addition to existing sets of functionalities of Application Programming Interfaces (APIs). This could be an additional opportunity, but there is a need for caution as possessing data belonging to data subjects may provide PIAs with mixed incentives and undermine their fiduciary obligation towards data subjects.

(d) Data subjects should be able to monitor the use of their data

The last element of controlling is a monitoring function which, as discussed, needs to be implemented by a combination of transparency and advice provided by PIAs. This is absent in the GDPR, but could be done by extension of the right of access.[1031] This right allows individuals to receive the standard set of information (including categories of data and the purposes of their processing) and a copy of the personal data undergoing processing, which may be provided in a ‘commonly used electronic form’. Also, the wording of recital 63 suggests that the right of access may be treated more broadly than in the DPD, because the rationale for the right described therein now points to awareness of the individual (and not accuracy of data). It is explained there on the example that access to data is given for their

[1030] Article 29 WP (WP 242 rev01) 2017, pp.17–18. Also, GDPR, recital 68.

[1031] GDPR, Article 15.

substantive value for the data subject.[1032] However, the access request may take up to three months to be executed,[1033] and subsequent repeated requests may be legally rejected.[1034] These limitations seem to be not justified in the case of online service providers who process data in a fully automated way, especially when they are able to trade personal data within milliseconds.[1035] So, access rights need to be reinforced to be a monitoring function of privacy management.

A reinforced right to access data should be more precisely formulated and should point to the standardised categories of data and data uses, use of interfaces (User Interface and API) to service providers' ICT systems, and PIAs as intermediaries. The main idea of PIAs (as described in Chapter V) is not to put them in the flow of personal data, but to put them in the flow of management data – data which control the flow of personal data between data subjects and data controllers. This may result in some duality, because the standard set of information (management data) would be available via UI and API, but raw personal data would be available only directly through UI. Alternatively, there should be some other safeguards preventing PIA from having access to personal data or otherwise eliminating incentives to process those data and monetise them.[1036]

Notwithstanding that limitation, the PIAs should be able to deliver a range of monitoring tools to their customers (ie data subjects). These tools, as discussed in Chapter VI, should include passive monitoring so, as a minimum, access to the statistics about data use, and more detailed logs about external use (the use of personal data for the purposes related to third parties). This may be extended by providing analysis of data use which may be derived from putting together statistics from many service providers over a longer period. Moreover, there may be active monitoring tools which rely on automatic notification about different activities related to data.

[1032] Which gives hope for a change of the narrow interpretation of the right of access which was presented in Case C-141/12 *YS* [2014] CJEU.

[1033] GDPR, Article 12(3).

[1034] GDPR, Article 12(5).

[1035] Between the click on the web link by the user and downloading the page contents.

[1036] Also, transmitting all data across the network and amassing them in one place would create unnecessary risk for data subjects.

Such activities may be a result of data breaches, data disclosure, or a sudden increase of their use.

From a legal perspective, it is important to secure the creation by service providers of reliable data about data use (statistics and logs), and access to these data by the means of API.[1037] Service providers should also generate automatic alerts (towards PIAs) in specified cases (eg data breach). This should be done by putting relevant obligations on service providers. However, in this area there is a need to go beyond legal obligations and carry out additional research in tamper resistant audit logs.[1038] The reliability of such solutions may be guaranteed by additional legal obligation or relevant security certificates.

So, the gap in regulation facilitating the controlling function of PMM can be closed by adding several features to the GDPR. Firstly, and probably most importantly, the law should enable a separate path of authorisation of data processing by the means of PIAs and individual privacy policies, obligatory for activities considered risky for individuals. This solution should be open to other applications as there are many potential opportunities for such individual policy. Also, law should make sure that the individual privacy policy is binding for service providers in all their activities and that users are secured from third-party tracking. Secondly, there is only some potential for simplification of the GDPR's right to erasure and broadening the scope of data portability to include more personal data. It also seems that PIA might act as a middleman for such activities, as they would have necessary relationships and expertise. Furthermore, monitoring functions could be implemented by the extension of the right of access. Such a reinforced right should be more precisely formulated and should point to the standardised categories of data and data uses, use of interfaces (UI and API) to service providers' ICT systems, and PIAs as intermediaries. It should foresee passive and active monitoring tools which rely on automatic notification.

It is time, now, to describe the gaps in organising.

[1037] Note, that there are deficiencies of technology in this respect which need to be compensated with accountability.

[1038] See Chapter VI.

2. *Closing gaps in organising*

The organising function of privacy management (ie having data organised for management by individuals) seems to be largely underdeveloped in the GDPR. At first sight, obligations to provide information seem to follow some schema. As noted above in relation to controlling, there is a 'standardised' data set which should be provided to data subjects at the beginning of processing (and in result of the access request) which gives some structure for organising data. When data are obtained from a third party, data subjects gain information about the purposes, information about categories of data, and an indication of the third party being the source of data. However, for unknown reasons, the information about data categories is not given when data are obtained directly from data subject.[1039] Furthermore, none of this allows individuals to gain a comprehensive picture of what data categories are processed and how they are used. The problem in providing such a picture lies mainly in the lack of standardised data categories and uses. Although some data categories are specified in the regulation (broad 'sensitive data', data concerning health, genetic data, biometric data, or data received directly from data subject),[1040] they are distinguished only for the purpose of applying to them different (usually more restrictive) rules, but not for the purpose of giving data subjects transparency (necessary for planning and controlling under the PMM model). Also, it is likely that categories defined by service providers will be incomparable with categories provided by other service providers, or even not meaningful at all.

The organising function of privacy management in the GDPR is even more underdeveloped in respect of data uses. This is because the GDPR keeps defining the way data are used through the lens of purpose specification, within the purposes declared by data controllers. This was extended already in the DPD[1041] to "specified, explicit and legitimate" purposes with indirect permission for additional uses 'compatible' with initial purposes.[1042] However, national laws

[1039] Which seems to be a deficiency of Article 13, because even if data are obtained directly they may still be collected in a way in which data subjects have no idea about their categories.

[1040] Which can be expanded by additional categories from ePrivacy Directive, such as location data, or traffic data; however, those categories are no longer distinguished in the proposal for new regulation substituting ePrivacy Directive, European Commission ("Proposal for a Regulation on Privacy and Electronic Communications") 2017.

[1041] GDPR keeps this extension.

[1042] DPD, Article 6(1)(b).

were broadly divergent in explaining the 'specificity' of the purposes and their 'compatibility'.[1043] According to Article 29 WP, 'specificity' means that "the purposes must be precisely and fully identified to determine what processing is and is not included within the specified purpose".[1044]

It is useful to exemplify this problem by using the following description of the purpose of data processing from the T&Cs of the biggest online social network.[1045] The statement below is apparently compliant with the DPD[1046] and will probably be compliant with the GDPR, as the GDPR contains only a small change in this respect, specifying that consent may be given for one or more specific purposes.[1047]

> **Provide, improve and develop Services.** We are able to deliver our Services, personalize content, and make suggestions for you by using this information [MB: this refers to all sorts of information from or about individuals listed in the previous point] to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services.

The problem in this description of purpose is its ambiguity on many levels. This is to say:

- 'Services' are defined as all the service provider's brands,[1048] products, and services directed to any of its customers (to data subjects, but also to advertisers and other third parties) which are (or will be) in its offer;
- 'content' is undefined. It may mean everything which is seen, including advertisements;
- 'personalisation of content' may mean the internal use of data to make the content more relevant to a particular user, or the external use of data[1049] to make the content or advertisement profiled for the user for other reasons, depending on paying partners' wishes;

[1043] European Commission 2003, pp.8–9.

[1044] Article 29 WP (WP 203) 2013, p.39.

[1045] "Facebook - Data Policy" n.d. Emphasis preserved.

[1046] It is an element of T&Cs available for European users in July 2017.

[1047] GDPR, Article 6(1)(a).

[1048] Note that it may also refer to the third party's product under the service provider's brand.

[1049] The external use of data is described in other, similarly broad part of T&Cs.

- ‘making suggestions’ covers not only all types of marketing advertisements, but any kind of suggestion by, for example, profiling the content in users’ news feed to back up a particular political opinion, or trend;
- ‘understand’ means that the data are analysed;
- ‘how you use and interact with…’ means any kind of relation between the user and group of concepts described in the second part of the sentence,
- ‘people or things you’re connected to and interested in on and off our Services’ equals everything which is somehow related to the data subject.

This sort of purpose description seems to not meet the criteria described in the Article 29 WP opinion. Despite the apparent specificity it covers every possible use of data by the service provider (or even under its brand) which may consist of profiling and suggestions based on analysis of all relevant data about data subjects’ interaction with anything (people, things, ideas) both inside and outside of the online service. This is quite a clear example in which the purpose limitation principle fails completely.[1050] What could the organisation function of PMM change in this?

(a) Data should be organised in a way which enables visibility of all data types and uses by data subjects

The example above shows that purpose limitation does not organise data uses for privacy management and that it is hard to expect it to work without changes.[1051] This is a problem for both sides of data processing, because the elasticity in the purpose specification is also a key element for Big Data, which, as discussed in Chapter IV, relies on data reuse. Currently this is often not possible without an additional consent procedure. It would be possible to overcome this problem with the organisation of data and data uses in a way presented in detail in Part C of Chapter VI.

So, following the discussion there, the best approach is to apply thematic division of data categories which would be as simple as possible. Such division should form the highest level of hierarchy and be extendable to new categories. The list of possible data uses should be much

[1050] Cf Čas 2011, pp.149–152.

[1051] On top of this, there is also a problem with vagueness of the provision in Article 6(4) of the GDPR related to assessment of compatibility of purpose of ‘further processing’.

shorter. Such categorisation is also possible on a general level and should be based on the level of risk introduced by data processing. Similarly to data categories, data use categories should also be extendable or split into more fine-grained choices.

Having defined data categories and data uses, the law should prescribe making the choice available for the combination of the above, ie any data categories per any data use. In this way, data subjects could have the basic blocks for building their privacy policies. This may lead to the user interfaces similar to those presented in Chapter VI.

(b) Data subjects should be able to control their data and policy by the means of standardised User Interface (UI) and Application Programming Interface (API)

Provision of interfaces, another basic building block of PMM, is not present in the GDPR, but there are some elements related to User Interfaces (UIs). That is to say, recital 63 describing explanations to the right of access to data suggests: "[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data". Another possibility is the already mentioned provision of information "in combination with standardised icons".[1052] These are, however, only indications that in some cases the user interface would be the less burdensome way of providing users with necessary information. Additionally, there are some obligations on service providers to receive requests sent with electronic messages and respond similarly, "by electronic means",[1053] or even in a response to the request of access in "a commonly used electronic form".[1054] Similarly, the right to data portability relies on 'transmitting' data to a new service provider. This cannot be done without an electronic interface to exchange data. All of this, however, looks more like introducing the elements of regular business activities from the second decade of the 21st century rather than introducing elements of data organisation.

The organising function requires more – interfaces to remotely manage personal data and their uses. So, service providers should be mandated to provide data subjects and PIAs with such

[1052] GDPR, Article 12(7).

[1053] GDPR, recital 59 and Article 12(3).

[1054] GDPR, Article 15(3).

interfaces. This is not a completely new discussion in data privacy law, as the implementation of the right to data portability on a mass scale requires similar functionalities.[1055] Similarly, the GDPR gives the possibility of exercising the right to object "by automated means using technical specifications", so by the means of UI.[1056] The UI seems to be easier to achieve, because it may be built in a web technology as an extension of 'privacy dashboards'.[1057] The API, however, requires more attention, because it needs to provide a whole set of standard functionalities enabling secure communication between service providers and PIAs to exchange between them data related to different users. API will be used to transmit mainly management data (data about privacy settings), but those data undoubtedly will be also personal, as they are related to particular individuals. A standard API needs to be developed for such use. The main functionalities of such an API are remote reading of privacy preferences by service providers and PIAs, and remote setting privacy preferences by the PIAs. Additionally, service providers should enable the PIAs (by the means of the API) to access the statistics about internal data use and more detailed logs about external use (so the use of personal data for the purposes related to third parties).

Based on those functionalities the interface project should develop scenarios of use (use cases) and define technical specifications for the main functions (methods) available for both sides of the connection. The main idea is to keep the simplicity of the service for data subjects. A data subject having the 'account' in one of the PIAs does not need to configure privacy settings for each new service provider, but only to point that service provider to their existing account in the PIA. From this point, following the successful authorisation of the parties, the service provider should securely receive from PIA the information about the data subject's privacy choices in a given area of service. Then, the service provider should set internal privacy preferences according to the received information and allow the PIA to monitor status, statistics, and remotely change settings. Such a set of functionalities does not seem to be overly complicated, but it needs to be developed according to the rules of interface (and protocol) planning. Most probably some of the existing protocols may be reused in such project.

[1055] Cf Article 29 WP (WP 242 rev01) 2017, pp.15–20.

[1056] GDPR, Article 21(5).

[1057] This, however, does not end the implementation, as categorisation of personal data and their uses need to be implemented throughout the back-office systems (as described in Chapter VI).

In conclusion, the organising function of privacy management seems to be largely underdeveloped in the GDPR. As shown in the example, vaguely described data types and purposes of processing pose a large problem for informational autonomy. To solve it, the types of data and data uses as defined in Chapter VI should be put into the law allowing data subjects to compose their privacy policies from their combinations. Also, the law should foresee using interfaces in direct relation to data subjects (UI) and in relation to PIAs (API). UI seems to be easier to build, but the specification of API needs to be defined by an appropriate technical body.

3. *Closing gaps in planning*

Planning is almost untouched by the GDPR, as the concept of an individual privacy policy simply does not exist there (or in any other privacy laws). It seems that legislators did not recognise the fact that for individuals the burden of giving consent comes from answering the same (or similar) questions over and over again for every service provider and for each of their services. That is simply inefficient and ineffective.

Also, it seems that legislators have no concern about changes in service providers' T&Cs over time. Changes in T&Cs are an important problem because currently the definitions of purposes and sets of choices that data subjects have as to the use of their data are based only on service providers' T&Cs. Service providers have a free hand to change T&Cs and do it quite often,[1058] usually without informing data subjects. This may change important factors of personal data processing, such as data categories, uses, level of disclosure, or authorisation. An illustrative example may be found on Google's website, which preserves the list of updates to their privacy policy.[1059] For example, within those changes are the following (additions in text are marked by italics, deletions are struck through):[1060]

[1058] For example, according to what is disclosed on Google's website, between 2015 and 2017 there were 11 policy changes: five privacy policy changes in 2015, three in 2016, and three in 2017 (until 7/10/2017).

[1059] See Google ("Updates: Privacy Policy") 2017. Transparency in this respect may indicate both good will of the company, and the fact that they see nothing wrong with such changes.

[1060] Google ("Updates: Privacy Policy") 2017.

- change implemented on 23 March 2014 which added to T&Cs the possibility of exposing individuals' personal data to third parties:

  > We *and our partners* use various technologies to collect and store information when you visit a Google service …

- change implemented on 19 December 2014 which added the possibility of collection of location data for any Google services, and increased the declared scope of collected data and sources of collection (enabling in this way to turn each user's terminal into Google-controlled collection device spying on other network users):

  > When you use ~~a location enabled~~ Google services, we may collect and process information about your actual location~~, like GPS signals sent by mobile device~~. We~~ may also~~ use various technologies to determine location~~, such as sensor data from your device~~ *including IP address, GPS, and other sensors* that may, for example, provide *Google with* information on nearby *devices,* Wi-Fi access points and cell towers.

- change implemented on 19 December 2014 which declared intrusion into content of users' communications:

  > *Our automated systems analyse your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.*

- Change implemented on 19 August 2015 which declared that Google obtains data about its users from third parties:

  > Information we collect when you are signed in to Google*, in addition to information we obtain about you from partners,* may be associated with your Google Account.

- Change implemented on 28 June 2016 which removed the statement about not linking cookie data collected by the means of external ad serving service acquired by Google with other personal data already collected by Google:[1061]

  > ~~We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.~~ *Depending on your account settings, your activity on other sites and apps may be associated with*

[1061] Note the use of the term 'cookie information' to describe data in cookie files which contain unique identifier attributed to a device and browser (and, hence, are capable to identify an individual) in opposition to 'personally identifiable information'.

> *your personal information in order to improve Google's services and the ads delivered by Google.*

These examples explain the problem in its entirety: the service provider changes the declared categories of data and data uses by changing the T&Cs. Therefore, the information received by data subjects at the time when they were subscribing to the service is no longer valid. In some countries Google informs users about changes in privacy policy by the means of a banner on the website of the service taking them through the list of changes. But, the problem is that such changes do not just need more information, but they should not be unilaterally imposed. Planning requires stability and this cannot be delivered when definitions of data categories and purposes are like sand castles.

(a) Data subjects should be able to define and change their own policy

A policy may be understood on a low level as a particular set of privacy settings (choices as to particular data categories and uses), which enables data subjects to manage their privacy for one or more online service providers. A more effective and convenient solution than reiterating consent is to centralise those individual privacy settings and let data subjects benefit from technology without unnecessary hassle related to consent.[1062] This is because, as shown in the previous chapter, technology can meet and respect their privacy expectations if only they are properly formulated and made known to the service providers.

Furthermore, there is no legal problem with such an approach. This is because the legal construction of an individual privacy policy can be as simple as the legal construction of purpose limitation. That is to say, while the purpose limitation mechanism relies on consent and waiver, an individual privacy policy can operate in the same way. So, the settings of an individual privacy policy presented to a service provider can waive individual rights to data within the scope of predefined (standardised) data types and uses (purposes). The only thing law has to do in this respect is to define data types and uses and enable the business model in which an individual privacy policy is accepted and respected by service providers.

[1062] More in Chapter IV.

So, the policy settings of service providers should be made available by the means of the Application Programming Interface. However, much can be done on top of this by the PIAs. For example, they can provide some high-level, default, pre-defined, and, importantly, not biased settings for different types of privacy profiles. This can be, for example, tailored to particular type of data subjects to which given PIA aims to provide the service (eg ethnic or sexual minorities). Management of such settings over time gives further opportunities. It may be useful to define additional limits on processing in particular times and in particular areas. For instance, some people would like to delete old behavioural data and not expose themselves to new data collections while others may be more open in this respect. Another potential key success factor of PIAs in the market would be their response to data-related events. Their system could, for example, react to a sudden increase in data use or to inaccuracies detected in the systems of the service provider (ie the PIA acts as a watchdog). This may be related to the results a person would like to achieve in the long term (anything from high profile to seclusion), or in reaction to a particular events, such as sudden increase of unwanted popularity or a data breach. Furthermore, PIAs should provide data subjects with independent advice and expertise in tuning those settings and also in changing them in response to different outcomes from monitoring. As PIAs compete against each other,[1063] they should have an incentive in providing their existing customers, data subjects, with the best possible service and growing their own reputation to attract new ones.

(b) Data subjects' policies should be stable (preserved and guaranteed)

Once the individual policy is not stored in the service provider's ICT environment, its stability may be achieved by obligating the service provider to respect its settings together with implementing enforcement and accountability tools. In this way, data subjects may by the means of their PIAs monitor their privacy settings. Furthermore, it is possible to operationalise the introduction of new services which may be related to the collection of new data types and new data uses. In this respect, the API should foresee some form of notification and the rest depends on the PIAs and user preferences. For example, it is possible to set some default treatment for new data and new data uses, or bring this fact to the attention of data subjects at

[1063] If they are not subsidised by state or private funds.

the first opportunity. In this way, extensions of service would not be burdened with the need to collect additional consent requests or risk stretching the limits of purpose 'compatibility'.

It is worth noting that resolving the problems of T&Cs changes in this way seems less burdensome than additional obligations relating to changes to such documents. The latter approach was developed, for example, in the case of European telecommunications services, where any changes to T&Cs have to be notified to users and an additional opportunity given for data subjects to withdraw from the contract.[1064] This led to situations in which there was no room for improvements in T&Cs, such as correcting simple errors or adding new services. Similarly, forcing customers to read screens and screens of additional information written in vague legalese, as practised in Europe in the case of changes to Google's T&Cs, seems to be simply not fit for purpose, for the same reasons as consent is not adequate to decide about a process. This could be avoided by putting the settings relevant to data subjects on the servers of PIAs and giving service providers a free hand in changing the rest.

So, planning is almost untouched by the GDPR, as neither the concept of an individual privacy policy nor requirement for stability of T&Cs exist there. The policy settings of service providers should be therefore made available by the means of the API. The only thing law has to do in this respect is to define data types and uses and enable the business model in which the individual privacy policy is accepted and respected by service providers. Once the individual policy is not stored in the service provider's ICT environment, its stability is much easier to achieve with the help of enforcement and accountability tools. In this way, data subjects may by the means of their PIAs monitor their privacy settings.

C Closing the Legal Gaps - Necessary General Legal Requirements

The previous Part has shown how to implement the particular elements of three basic functions of PMM: controlling, organising, and planning on top of the GDPR, the most advanced data privacy law so far. They, however, also require some general legal rules to support their operation. The first rule, discussed in section 1, is an overarching principle (legal right) which is necessary for the proper functioning and robustness of the applied regulatory mix. Section

[1064] Directive 2002/22/EC (Universal Service Directive), Article 20(4).

2 then presents why the new laws should have an extraterritorial reach and how this should be shaped. Finally, sections 3 and 4 discuss a few constraints which need to be put on the scope of regulation, on the actions of Personal Information Administrators, and on service providers to precisely address the regulation to existing and possible problems.

1. *Enacting an overarching principle of informational self-determination*

As presented in Part A, there is currently no substantive legal entitlement which could secure the power of the individuals to effect privacy management. Also, the conclusion about the procedural approach of FIPPs was that they reflect a 40-year-old balance of some higher level values described in the language of procedural limitations. Because this balance is no longer relevant in the current context, it needs to be either recast, or a substantive principle describing the interest of individuals needs to be implemented at a constitutional level. Such a principle should be a normative entitlement to the positive liberty which was presented at the outset of this thesis in Chapter II and used to identify privacy problems in Chapter III. Such normative entitlement is the right to informational self-determination.

(a) Why the right to informational self-determination is necessary

Such a substantive principle, the right to informational self-determination, is necessary for effective regulation. Firstly, given that personal data are stored on the premises of service providers and the balance of power is tilted heavily towards them, individuals need strong entitlement to their data.[1065] Such a right should clearly and understandably define their interests in their data and help in the interpretation of the whole bundle of lower-level data privacy laws. That is to say, the overarching right should allow data subjects to require service providers to perform all actions enabling privacy management and related to controlling, planning, and organising.

[1065] Lack of such an entitlement may be seen as the biggest weakness of data privacy laws, Laudon 1996, p.97. The right to informational self-determination exists only in Germany, as explained in Chapter II. See also subsection (b), below, about the scope of this right.

Secondly, statutory rules regulating those functions may be seen as separate elements of procedure and, therefore, may erode in time in the same way as the consent or purpose specification principle. Having a substantive right to informational self-determination underpinning the data privacy rules and guiding how they should be applied would prevent such erosion, so the outcome of the regulation could be more coherent.[1066] This is because low-level rules would be explained and applied as smaller elements of a larger concept of underpinning freedom, having in mind their purpose and not just the wording. The result would also be more likely to be flexible with regard to the further development of technology. For these reasons it is hard to overemphasise the significance of such overarching right pertaining to all phases of data processing and to all aspects of privacy management.

In the EU, the freedom for individuals to make decisions about their data needs to be secured at the constitutional level. This is because the legal system of the EU is based mainly on continental law where laws are hierarchical and applied top-down, starting from the highest level of constitutional principles. In such a system the right to informational self-determination should be defined at the highest level where this norm would be weighed against other principles at the same level, such as the European freedom to conduct a business.[1067] Currently, the right to the protection of data in Article 8 of the Charter of the Fundamental Rights of the European Union (ChFREU) in the case of conflict with another fundamental right is balanced twice. This is because its principles of fairness and legitimacy taken from FIPPs are already the result of a balancing exercise (ie they already balance privacy interest with the interest of data users in eg 'free movement of data').[1068] So, in the case of conflict, they would be balanced second time according to the principle of proportionality established in Article 52 of the ChFREU. A new principle of the informational self-determination substituting Article 8 of the ChFREU could eliminate this vagueness.

Having said that, the traditional common law approach is significantly different. It does not foresee the enactment of fundamental rights, but rather recognises a 'residual liberty' which

[1066] Albers 2014, p.214.

[1067] See Article 16 of the ChFREU.

[1068] See row "0" in Schedules A and B, and Part A above. Cf other idea about broad scope of Article 8, but also a need to establish an interference (similarly as in the New Zealand system) in Hustinx 2013, p.18.

consists of everything which is not expressly forbidden.[1069] For example, the Younger report agreed that a general right to privacy may be desirable, but a statutory declaration of such law "has not been the way in which English law in recent centuries has sought to protect the main democratic rights of citizens".[1070] In spite of (or along with) this traditional view, most common law countries adopted some form of the continental approach recognising positive lists of rights.[1071] But, the position of privacy rights is not as strong in these jurisdictions. For example, in New Zealand privacy is not included in the Bill of Rights, but was recognised by minority as "other common law right".[1072] In the case of Canada, privacy is interpreted as a part of the right to be secure against unreasonable search and seizure,[1073] which unfortunately concentrates its application only on the (vertical) relation between state and its citizens.[1074] Only in the UK, being under the influence of the European continental system, the right to respect for private and family life was introduced as one of the 'Convention rights' set out in Schedule 1 to the Human Rights Act 1998 (HRA). Also, as a member of the European Union,[1075] the UK (still) recognises the rights contained in Article 7[1076] and Article 8[1077] of the

---

[1069] Turpin and Tomkins 2007, p.728; as per Sir Robert Megarry V-C in *Malone v Commissioner of Police of the Metropolis (No 2)* [1979] Ch 344.

[1070] Committee on Privacy, Home Office 1972, para.35.

[1071] There is no such legislation in Australia on the federal level. However, two Australian states enacted their versions of bills of rights: Human Rights Act 2004 (ACT), Charter of Human Rights and Responsibilities Act 2006 (Vic).

[1072] Eg s 28 of the New Zealand Bill of Rights Act 1990 (BORA) recognising other possible rights not affected by the enactment of BORA and minority opinion in *Allistair Patrick Brooker v The Police* [2007] NZSC 30, paras213–228 as per Thomas J.

[1073] Krotoszynski, Jr. 2016, p.44; Penk and Tobin 2016, p.119; Law Commission (NZLC IP14) 2009, para.4.118.

[1074] *RWDSU v Dolphin Delivery Ltd.* (1986) 2 SCR 573 (SC), para.36; also, *Eldridge v British Columbia (Attorney General)* (1997) 3 SCR 624 (SC), para.35; also Krotoszynski, Jr. 2016, p.42; furthermore, if the agents being private actors obtained information acting in the regular scope of their duties and handed it to police, no seizure nor search has occurred, Bailey 2008, p.285.

[1075] On 29 March 2017 the UK officially triggered the Article 50 (of the Treaty on the European Union) procedure to leave the UE. This means, according to Article 50(3), the UK will be a member of the UE until the (currently negotiated) treaty on leaving enters into force, but no longer than two years from the notification (so by 29 March 2019). The European Council may prolong this term by the means of a unanimous decision (taken with the UK).

[1076] The right to respect for private and family life.

[1077] The right to the protection of personal data.

ChFREU and the UK courts should ensure compliance with them.[1078] So, the chances that a new constitutional-level substantive privacy principle appears in any of these countries are slim. Instead, the viable option in these countries seems to be to enact such a principle on the statutory level.

Taking all of this into account, this thesis presents below a proposal for a right to informational self-determination and shows how it could possibly fit into existing constitutional-level European rights. This exercise is undertaken because such a principle is necessary and the regulations described in this thesis have the most chance of success in the EU.[1079] However, the question of how to implement this right is left open. Amendments to the ECHR, ChFREU, or Convention 108 are possible, but require the normal procedure of amendment of an international treaty. As indicated above, another option, perhaps the only one for common law countries, is to enact such a principle on the statutory level. What should such a principle exactly look like?

(b) What the right to informational self-determination should look like

The right to informational self-determination should ideally be expressed as the following:[1080]

> Everyone has the right to determine for himself or herself whether personal data concerning him or her may be collected and disclosed and how they may be used.

This particular formulation was proposed as a draft right to data protection during the Convention preparing the draft of the ChFREU by the Convention's Praesidium.[1081] But, at that time the members of the Convention were not ready to define such a fundamental right,

---

[1078] Despite the Polish–British protocol on the application of the ChFREU (No 30, so-called 'opt out'), Case C-411/10 *N. S. v Secretary of State* [2011] CJEU, para.120.

[1079] See Chapter IV and below.

[1080] Article 19 of the draft Convention (CHARTE 4360/00) 2000, p.25; cf 'individual control principle', The White House 2012, p.11; also, Council of Europe proposed reinforcing privacy with "the right to control one's own data", point 5, Parliamentary Assembly of the Council of Europe (Resolution 1165) 1998.

[1081] Led by the Convention's President Roman Herzog, the former head of the German Federal Constitutional Court.

so they focused on a different version reflecting the compromise they had achieved during previous legislative processes. [1082]

However, that different version, the right to data protection as formulated in Article 8 of the ChFREU, is a protective right without any protected value or liberty. The definition does not explain what aspects of an individual's position or actions are safeguarded by 'data protection'.[1083] This is a problem, because it shifts the subject of protection from individuals to the "concerning them data", which do not have any value or interest per se.[1084] In addition, the ChFREU lists in Article 8(2) the principles of data processing (some of FIPPs) and some auxiliary rights (such as the right of access to data), but it remains unclear *why* personal data are protected. In other words, the right to data protection fails to express the substance of the relationship between data and the data subject as a person. Instead, it concentrates on procedure.

Contrary to that, the wording of the right to informational self-determination quoted above captures the essence of the individual entitlement to data and defines a positive liberty to make decisions about the collection of data and their uses. This is the substantive freedom which is (or should be) protected. The scope of this freedom can be built on the bases of relevant decisions of BVerfG and contains all elements discussed in Chapter II.[1085] That is to say:[1086]

[1082] The current wording of Article 8 is based on the Article 286 of the Treaty establishing the European Community (currently Article 16 of the TFEU), DPD, ECHR, and Convention 108, Convention (CHARTE 4423/00) 2000, p.8; also, Cannataci and Mifsud-Bonnici 2005, p.10.

[1083] Cf "the Fallacy of Necessity" in Brownsword 2009 pp.90–92.

[1084] See Zanfir 2014 p.245 citing Norberto Nuno Gomes de Andrade.

[1085] Note that this scope differs slightly from the German right to informational self-determination and is based on three decisions: *Census Act* [1983] BVerfG; *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG; *Nuremberg Higher Regional Court* [2013] BVerfG.

[1086] Cf Barnes 2016, p.303 who seems to indicate that informational self-determination is a legal position resulting from the sum of data subjects' rights; also, view of data protection as a tool for the preservation and promotion of the value of autonomic self-development and political participation, Rouvroy and Poullet 2009, p.50.

- Information security (understood as its integrity and confidentiality),[1087] which is a necessary prerequisite to any further determinations relating to data;
- Knowledge (the ability to ascertain what of a data subject's information is known to whom),[1088] which may be understood as awareness of collection of data, purposes and their actual use;
- Autonomous choice itself (freedom to decide "whether to engage in or desist from certain activities").[1089]

The proposed wording protects all these things and also covers the horizontal aspect of the application of the right. That is to say, this right should form an entitlement in private law contractual relations. The reason for this is to prevent individual "self-determination from being subverted into a determination by others" in the context in which those "others" have the influence and ability to de facto determine unilaterally the contract terms.[1090] This supports the view that individuals cannot just have 'all or nothing' choice, but need to be continuously involved in data processing.[1091] This also answers the concern about manipulation of the IT system itself and the data stored in the system,[1092] as the consequence of such manipulation would be to undermine the decisions of an individual and his or her control over data.

(c) Can it be developed in Europe?

Although such a right does not exist at the constitutional level in Europe,[1093] it is possible that it may develop on the basis of existing rules. There are some indications that this may happen.

[1087] *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG, paras204–205; note that they are, together with availability, the main components of information security triad, which is an established conceptual model of computer security, Cherdantseva and Hilton 2013, p.547; also, ISO/IEC 27001:2013, p.v.

[1088] *Census Act* [1983] BVerfG; Bröhmer and Hill 2010, p.148.

[1089] Note that the wording from Bundesverfassungsgericht 1983 was extended by explicitly adding 'collection'. Cf Bröhmer and Hill 2010, p.148.

[1090] *Nuremberg Higher Regional Court* [2013] BVerfG, para.20.

[1091] Mayer-Schönberger 1997, pp.229–230.

[1092] *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG, paras204–205, 240.

[1093] Only in one Member State - Germany. Also, the informational self-determination surely had influence on the European law and there are voices that much of the DPD was derived from this principle, see Mayer-Schonberger 2008, p.730.

Firstly, the scope of "data relating to the private life of an individual"[1094] recognised in the jurisprudence of Article 8 (the right to respect for private and family life) of the European Convention on Human Rights (ECHR) and the scope of data which are 'personal', so relating to an identified or identifiable individual[1095] under the EU data protection regime are overlapping and close to each other. Although data protection prima facie seems to cover more data because it is easier to find a relation to individuals than to their private life,[1096] the difference between them depends only on the perception of what is private and on the interpretation of the role of social interest. This is because it may be argued, as did the BVerfG, that "unimportant data no longer exist" in the context of ICT,[1097] so in this context all personal data are, in a sense, private. Some personal data are being disclosed by data subject not because they are not private, but because the data subject decided so, or because there was a social interest in such disclosure (which trumped one's privacy interests).

Secondly, such a view may be reinforced by the observation that the European Court of Human Rights (ECtHR), has recognised personal data of 'different flavours' as a part of the Article 8 right to respect for private life. In this respect, it was held that storing and processing data broadly related to the individual is enough to interfere with individual rights.[1098] Also, Article 8 covers inter alia: metadata such as records describing phone conversations,[1099] photographs or videos,[1100] voice samples,[1101] location data,[1102] which all should not be used without consent

[1094] Eg *Amann v Switzerland* (*2000)* ECtHR, para.69; also, Gellert and Gutwirth 2013, p.526.

[1095] DPD, Article 2(a). And, Convention 108, Article 2(a).

[1096] This may be observed, for example, in the decision Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof v Osterreichischer Rundfunk* [2003] CJEU, paras68–70 where the Court moves from the processing of personal data to the processing of the personal data liable to infringe fundamental freedoms; also the German *North-Rhine Westphalia Constitution Protection Act* [2008] BVerfG, para.197, where distinction is made between collection of private data, and access to all data which facilitates creation of a comprehensive picture of the individual.

[1097] Bröhmer and Hill 2010, p.149.

[1098] *Amann v Switzerland* (2000) ECtHR, para.65; *Leander v Sweden* (1987) ECtHR, para.48.

[1099] Such as 'metering' the phone, *Malone v The United Kingdom* (1984) ECtHR, p.64.

[1100] *Von Hannover v Germany* (2004) ECtHR, paras50–53; *Sciacca v Italy* (2005) ECtHR, para.29.

[1101] *PG and JH v the United Kingdom* (2001) ECtHR, paras59–60.

[1102] *Uzun v Germany* (2010) ECtHR, para.52.

of the data subject,[1103] or outside the scope of the intended use.[1104] Furthermore, the jurisprudence of ECtHR recognises autonomy and self-determination as important principles underpinning Article 8.[1105] This includes "aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world".[1106] Furthermore, in recent cases this was extended to the right to control the use of the images because they are "essential components of personal development" and reveal "the person's unique characteristics and distinguishes the person from his or her peers".[1107] It seems that this argumentation all supports the idea of informational self-determination.

Thirdly, despite the fact that data protection is more proactive and even if it is assumed that it covers more data than privacy, both data protection and protection of data relating to the private life cover essentially the same interest of individuals. Although academics point to other interests or values covered by data protection, those interests or values are usually methods of protecting privacy or values protected by privacy.[1108] Also, European legislators reuse ideas relating to privacy for the goals of data protection, ie Privacy by Design and Privacy Impact Assessment, are renamed as, accordingly, Data Protection by Design and Data Protection Impact Assessment.[1109] Furthermore, the Court of Justice of the European Union (CJEU) after the adoption of the ChFREU considered the existence of two different rights there: the right to respect for private and family life (Article 7) and the right to protection of personal data (Article 8) and started to treat those two rights jointly. In *Schecke* the CJEU acknowledged that those two rights are "closely connected",[1110] that they jointly create "the right to respect for private life with regard to the processing of personal data",[1111] and simply

[1103] *Flinkkilä and Others v Finland* (2010) ECtHR, para.75.

[1104] *Verlagsgruppe News GmbH and Bobi v Austria* (2013) ECtHR, para.86.

[1105] Starting from *Pretty v The United Kingdom* (2002) ECtHR, para.61.

[1106] *Evans v The United Kingdom* (2007) ECtHR, para.71; also, *Odièvre v France* (2003) ECtHR, para.29.

[1107] *Reklos and Davourlis v Greece* (2009) ECtHR, para.40; also, *Von Hannover v Germany (No 2)* (2012) ECtHR, para.96.

[1108] Cf Hustinx 2013, pp.6, 51; De Hert and Gutwirth 2009, pp.6, 9; Rouvroy and Poullet 2009, p.70; Bygrave 2001, p.281; Zanfir 2014, p.244.

[1109] GDPR Article 25 (Data Protection by Design) and Article 35 (Data Protection Impact Assessment).

[1110] Cases C-92/09, C-93/09 *Schecke v Land Hessen* [2010] CJEU, para.47.

[1111] Ibid., para.52.

started to read them together. This approach was followed in successive cases: *Schwarz*,[1112] *Digital Rights Ireland*,[1113] *Google Spain*,[1114] *Ryneš,*[1115] and *Tele2*.[1116] With minor exceptions,[1117] the Court does not see separate interests nor separate rights.[1118] Such 'joint treatment' is criticised by the authors finding distinct protected interests,[1119] but it seems that the Court is undiscouraged by such critique and regards protection of privacy of data and data protection as one concept. In other words, the Court conflates the right to data protection and the right to privacy in the sphere of data (or information) into one instrument exposing a common interest underpinning both of them.

Therefore, perhaps Ockham's razor should be applied to define the right to informational self-determination as an aspect (or extension) of the right to respect for private life in the sphere of information.[1120] Adopting such a principle, as argued above, would not only explain the role of consent in this bundle of rights but also allow it to overcome its weaknesses (as has been shown in this thesis). Some authors are of the opinion that the concept of informational self-determination puts a great deal of emphasis on consent,[1121] which is only a partial truth. Consent is currently a well-known tool for controlling data, and those authors seem to put the

---

[1112] Case C-291/12 *Schwarz v Stadt Bochum* [2013] CJEU, para.25.

[1113] Case C-293/12 *Digital Rights Ireland Ltd v Ireland* [2014] CJEU, paras53, 65, 69.

[1114] Case C-131/12 *Google Spain* [2014] CJEU, paras69, 87, 99.

[1115] Case C-212/13 *František Ryneš* [2014] CJEU, para.28. Such joint reading of two rights has interesting dynamics. For example, in *Ryneš* the CJEU used the fact that both rights apply to narrow the derogations to data protection (as they may infringe the right to private life).

[1116] Cases C-203/15, C-698/15 *Tele2 Sverige* [2016] CJEU, para.100.

[1117] Case C-419/14 *WebMindLicenses* [2015] CJEU, para.79, where CJEU found that a legal person may claim some rights resulting from Article 8 ECHR, but its data cannot be personal within the meaning of Article 8 of ChFREU; also, Advocate General opinion to *Digital Rights Ireland* contains some discussion about relation between those two rights and finding that they have different scope, Pedro (Opinion to the case C-293/12) 2013, paras55, 61–67, 74. However, this Opinion seemed to have little impact on the final decision, where the Court applied 'joint reading'.

[1118] Cf also the idea of two separate rights for which the Court recognised a 'close link', Sharpston (Opinion to the case C-92/09 (*Schecke*)) 2010, para.71.

[1119] Hustinx 2013, p.51; also, Kranenborg 2014, p.230.

[1120] Cf 'conceptual link between privacy and data protection' in Kranenborg 2014, p.229; cf Rouvroy and Poullet 2009, pp.70, 78.

[1121] Hustinx 2013, p.50; Kranenborg 2014, p.229; but, cf other view that despite recognising the privacy interest as the informational self-determination consent needs societal control, Rouvroy and Poullet 2009, pp.72–73.

equality sign between informational self-determination and consent.[1122] Furthermore, they attribute the problems of consent to problems of informational self-determination understanding that applying informational self-determination would practically force people to constantly consent to every little piece of personal data generated by every move in a digital world.[1123] This is not correct. Applying this thought pattern without deeper reflection puts the laws in a cul-de-sac in which legislators are afraid of individual self-determination because of concerns related to consent.[1124] It is true that consent fails to deliver control over data because, as described in Chapter II, it is inadequate for the task of controlling the privacy process. However, consent is not the only option of implementing informational self-determination. Instead, privacy management may do this job properly, but it requires the normative definition of the right of the individuals which is capable of including all necessary activities. Such a normative vehicle is the right to informational self-determination. If it would not find its way into the constitutional-level norms of a given jurisdiction, it should be enacted as a general principle of the statutory law defining privacy management rights.

To sum up, it is hard to overemphasise the significance of an overarching individual right pertaining to all phases of data processing and to all aspects of privacy management. Such a right should have as high a place in laws' hierarchy as possible. It could secure the power of individuals to determine whether personal data concerning them may be collected and used, in a way which may be elastically adjusted to the new threats arising from the future developments of technology. It is a right which enables deemphasising procedural rules such as consent and introducing and securing effective methods of authorisation such as PMM.

2. *Extraterritorial reach of the law*

The complexity of issues relating to which law is to be applied to services in a global network, which DPA in which jurisdiction should have oversight over data processing, and, finally, which courts have jurisdiction to hear complaints, were recognised by the OECD Expert

[1122] Eg Buchmann 2013, p.21; also, Hustinx 2013, p.8.

[1123] Buchmann 2013, p.21.

[1124] Cf "defining informational self-determination claims too much and protects too little", Bennett and Raab 2006, p.9.

Groups[1125] and during work on Convention 108.[1126] But, the documents which were developed did not contain any specific rules to solve those problems. Rather, the works of these groups went towards minimising differences between jurisdictions and harmonising rules between them by creating "common core" principles.[1127] Although technically choice of applicable law and choice of jurisdiction are two separate aspects, in the practice of data privacy laws the rules of choice of law are often used as the functional equivalent of the rules of jurisdiction.[1128]

The core of the problem is that national data privacy laws can be circumvented by using the global data transmission network. This can be done either by providing services for data subjects directly from abroad (collection from abroad), or indirectly by transferring abroad data already collected in a given country (transfer). What can be called transfer and what is direct provision of services are usually blurred because they depend on legal rules, the location of data, equipment, or establishment of legal entities. While entities performing the transfer of information abroad are without doubt regulated by the national law (and national laws usually impose conditions on and restrictions to such transfers),[1129] entities providing services directly from other jurisdictions may be perceived differently.

This provision of services from abroad gives lawmakers a difficult choice. One option is to give up and agree that some (increasingly important) part of the services provided in a given country is subject to foreign law and, therefore, is exempted from local regulation.[1130] The second option is to work with that foreign country on the level of protection and resolution of complaints, which may be difficult if the other country does not perceive the need to regulate those services. The third option is to design one's own data privacy laws to be applied extraterritorially to service providers delivering services from abroad[1131] taking into account

[1125] OECD Guidelines 1980, paras24–76; OECD Guidelines 2013, p.111.

[1126] Council of Europe ("Explanatory Report") 1980, para.10.

[1127] OECD Guidelines 2013, p.102; Council of Europe ("Explanatory Report") 1980, para.20.

[1128] For example, Article 4 of DPD, or Articles 3 and 79(2) of GDPR. Also, Kuner 2010, pp.179–181; Case C-131/12 *Google Spain* [2014] CJEU, paras51–58.

[1129] Privacy Act 1993, pt 11A; Privacy Act 1988 (Cth), Australian Privacy Principle 8 and s 16c. DPD, Chapter IV.

[1130] Eg Law Commission (NZLC IP17) 2010, p.390.

[1131] 'Extraterritorial' may have many meanings, eg Colangelo 2014, pp.1312–1314. Here, extraterritorial reach of the law means the application of the national law to actions of entities providing services from another

that it may not be possible to fully enforce the legal obligations imposed on subjects without their local presence.[1132] This unfavourable effect is likely to be less significant when such service providers have sources of revenue in a given country.[1133] So, the third option is the one chosen most frequently. This point was already touched on briefly in Chapter IV, where it was identified that the extraterritorial effect of the law is an important policy issue and that ICT services are exported mainly from the US to other jurisdictions, which effectively exports low privacy standards from there to other countries.

The rationale behind choosing extraterritorial application of law is mainly a protection of one's own residents,[1134] but also the promotion of the higher level of protection abroad. A system in which the law applicable to trans-border services is the law of the country of origin triggers a 'race to the bottom'. This is because it gives an incentive for service providers to look for the jurisdiction which gives them the least risk for their operations. On the contrary, when law has extraterritorial reach (as described above) the service providers have to choose whether they provide their services to a given jurisdiction. If the higher standard is introduced by an economic area large and wealthy enough to be perceived as an important market, they will choose to implement higher standard regardless of the standard in their home country. However, this requires harmonisation between rules of transfer and rules of extraterritorial applicability to prevent circumvention of one by another.

Once this higher standard is implemented, it should be easier to extend the higher standard to other countries.[1135] Firstly, it is easier for service providers to apply one standard of services to multiple countries. So, keeping a lower standard for some jurisdictions may be not rational in economic terms (if it is not justified by additional profits from exploiting more personal data for those regions). Secondly, other countries will have incentives to follow and apply

---

jurisdiction. However, it may also be claimed that such application of the law is within the jurisdiction of that national law because services are provided in that jurisdiction.

[1132] Under international law there are certainly limitations for international jurisdiction due to the principles of state sovereignty and non-interference, but there is little agreement where they lie. There are no global instruments containing jurisdictional rules for data privacy. Kuner 2010, pp.185–186.

[1133] Eg Case C-131/12 *Google Spain* [2014] CJEU, para.51.

[1134] European Commission (SEC(2012) 72 final) 2012, p.25; Article 29 WP (WP 179) 2010, p.24; cf Bygrave 2014, p.201.

[1135] Bradford 2012, p.6.

higher standards. For example, DPD exerted influence on other jurisdictions by the means of limitations of the data transfer mechanism.[1136] As the transfer was more difficult to the country without the status of "giving adequate protection level",[1137] many countries (including New Zealand and Canada) interested in achieving such status made changes to their laws to bring them closer to the European one, which effectively exported the elements of the European legislative model to over 30 countries.[1138] Thirdly, once the higher standard is implemented by a global service providers it is significantly harder for them to apply many of the arguments denying the feasibility of reform.[1139] This is the path which should be recommended for application of PMM, mainly because this is currently the only possible way to enforce a privacy standard which is higher than the US standard.

There are, however, some legislative choices to be made to achieve this goal. Establishing a legislative jurisdiction requires some foreign element to be linked to the application of the laws 'across borders'.[1140] This linkage in the case of the DPD is processing data "in the context of the activities of an establishment of the controller on the territory of the Member State",[1141] or, in case of a lack of such establishment, "making use of equipment, automated or otherwise situated on the territory" of the Member State.[1142] This is somewhat unclear and in practice 'making use of equipment' is understood very broadly more as 'any means' (including technical and human intermediaries), which was construed on the basis of wording of other versions of the Directive, and its motives.[1143] Because of this lack of clarity and excessive broadness[1144] of the DPD, the GDPR makes it much clearer that it applies to any data

[1136] Ibid., pp.22–26.

[1137] Article 25. Alternatively, the transfer must be justified under one of derogations listed in Article 26.

[1138] Greenleaf 2012, pp.74–75.

[1139] Which were humorously described in Hoofnagle 2007.

[1140] Eg Kuner 2010, p.184.

[1141] Note that 'in the context' allows the law to attribute the responsibility for data processing to subsidiary of an overseas service provider when such a subsidiary does not process data by itself, eg Case C-131/12 *Google Spain* [2014] CJEU, paras55–58.

[1142] DPD, Article 4 (a) and (c).

[1143] Mainly recital 20 of the DPD and previous versions showing the intention of the legislator, Article 29 WP (WP 179) 2010, p.20; Bygrave 2014, p.201.

[1144] For example, the European law applies also to any use of equipment in the EU for processing data from third countries, more details in Article 29 WP (WP 179) 2010, p.21.

processing related to offering goods or services to data subjects in the European Union or monitoring of their behaviour.[1145] This, together with the right to bring claim to a court where data subject has his or her residence,[1146] sets the applicable law and jurisdiction to Europe.[1147]

Australia solved this problem in a somewhat similar fashion to Europe by a provision in the Privacy Act 1988 (Cth) declaring its extraterritorial application. The Act's application extends to acts done and practices engaged in outside Australia by an organisation or small business operator that has an "Australian link".[1148] Such an Australian link may be personal (eg Australian citizen, or Australian company), and may also be established on the basis of carrying on business in Australia and collecting or holding personal information in Australia. This seems similar to the European approach in the GDPR. Interestingly, the Australian Senate Committee presented during the legislative process a quite European view on this matter:[1149]

> 3.97 The committee notes that there may be some enforcement challenges relating to this provision, but does not consider that this reduces the need for this reform to proceed.

It seems that an Australian court would have no problem in establishing jurisdiction over a service provider from another country,[1150] but as far as the author is concerned there were no such privacy cases so far.

The question of extraterritorial application of the New Zealand Privacy Act 1993 is quite convoluted. The Act itself refers to this only in part by stating in s 10 in quite vague language the rule which seems to declare that privacy principles 6 and 7 (related to access and correction) apply to information regardless of the fact that it is held outside New Zealand.[1151] This could possibly be read as an extraterritorial reach of the Act, but, the Law Commission[1152]

[1145] GDPR, Article 3.

[1146] GDPR, Article 79.

[1147] With some negative consequences of this fact to service providers.

[1148] Privacy Act 1988 (Cth), s 5B(1A).

[1149] Parliament of Australia, Environment and Communications References Senate Committee 2011, para.3.97.

[1150] Eg *Duffy v Google Inc* [2015] SASC 170.

[1151] This is because the broad definition of agency does not exclude foreign agencies, Privacy Act 1993, s 2(1).

[1152] Law Commission (NZLC IP17) 2010, p.390.

and Privacy Commissioner[1153] have explicitly stated different views. To make this more complicated, the New Zealand commentators seem to agree that the *collection* of information in New Zealand by a foreign agency would be covered by the Privacy Act 1993.[1154] This means that there are three different opinions on this issue. Also, it seems that Government sees problems with cross-border outsourcing and transfers,[1155] but not with online services directly provided to NZ residents. This seems to be a substantially different approach than that taken in other jurisdictions. Also, New Zealand courts, unlike their Australian counterparts, are not willing to recognise local subsidiaries of overseas service providers as relevant defendants for claims against their mother companies.[1156] There are, however, other New Zealand statutes where extraterritorial application of the law was used (eg Fair Trading Act 1986).[1157]

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) is silent on its extraterritorial reach, but courts have stated that it should apply in such a way where there is a "real and substantial" connection with Canada.[1158] The court applied to PIPEDA the test previously used in cases involving an interprovincial and international element[1159] to disagree with the Canadian DPA that it did not have jurisdiction over some privacy claims. In this way, the Canadian DPA and courts started to apply PIPEDA extraterritorially, considering in the case of the Internet the following connecting factors:[1160]

(1) the location of the target audience of the website,

(2) the source of the content on the website (or the location of content provider),

(3) the location of the website operator, and

[1153] Office of the Privacy Commissioner n.d.; note that the position of the Privacy Commissioner about overseas application of Privacy Act 1993 changed during this period.

[1154] Gunasekara 2009, p.169; Toy 2010, p.225.

[1155] New Zealand Ministry of Justice 2014, pp.16–21.

[1156] *A v Google New Zealand Ltd* [2012] NZHC 2352, para.46.

[1157] Fair Trading Act 1986, s 3; more broadly, Toy 2010, p.224.

[1158] *Lawson v Accusearch Inc.* 2007 FC 125.

[1159] Ibid., para.34; the first application of this test in an international dimension, *Beals v Saldanha* 2003 SCC 72; also, the first use for interprovincial jurisdictional problems, *Morguard Investments Ltd. v De Savoye* (1990) 3 SCR 1077 (SC).

[1160] *A.T. v Globe24h.com* 2017 FC 114, p.53; the factors were originally used in copyright case *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers* 2004 SCC 45, para.61.

(4) the location of the host server.

For example, in the *AT v Globe24h.com*, the last factor, the location of the operator of the website and the website itself in Romania, was found the least important and non-conclusive as telecommunications occur "both here and there".[1161] Also, the principle of comity (invoked usually by defendants) was found "not offended where an activity takes place abroad but has unlawful consequences" in Canada.[1162] In this way, the Canadian solution seems to be (again) the most flexible one, as the court in each case needs to weigh the *forum non conveniens* argument.[1163] However, this solution may not be very reliable where courts are not eager to decide upon claims against overseas defendants (such as in New Zealand).

So, there is a practice of extraterritorial application of data privacy law (and jurisdiction of national courts) in all jurisdictions but New Zealand. The rationale behind this practice is mainly the protection of their own residents, but it also serves to promote a higher level of protection among other countries. Therefore, this is the recommended way for application of privacy management rules, and, currently the only possible one to enforce a higher privacy standard on foreign companies. The best way to implement such an extraterritorial reach should reflect the local legal system and culture, so will differ across jurisdictions.

3. *Keeping PMM within bounds*

(a) Limiting the scope of regulation

Measures described below aim to limit the scope of regulation implementing PMM to those entities which use personal data in a way endangering informational autonomy. There need to be such limitations, as data processing is an activity undertaken by most businesses and all governmental authorities. Even in the case of online service providers, the data processing activities of a local internet grocery differs significantly from the data processing of a large social network provider. As discussed in Chapter IV, there is no need for the proposed regulations to cover all activities related to providing online services. Indeed, it would be

[1161] *A.T. v Globe24h.com* 2017 FC 114, para.52; following *Libman v The Queen* (1985) 2 SCR 178 (SC), p.208.

[1162] *A.T. v Globe24h.com* 2017 FC 114, para.54.

[1163] *Lawson v Accusearch Inc.* 2007 FC 125, para.49; also, *Google Inc. v Equustek Solutions Inc* 2017 SCC 34.

improper, as the number of complex technical obligations would create a burden for those data controllers which do not infringe on informational self-determination. It may also be argued that such uniform regulation is already a problem for many companies in the case of the European law.[1164] So, it seems that the best idea for such regulation is a statutory instrument introducing lex specialis to data privacy laws (governing only a particular subset of activities). This instrument would introduce additional rules presented in this chapter for some data controllers specified below.

As discussed in Chapter IV, such lex specialis should focus on particular groups of businesses which could potentially breach informational autonomy. That is, those who use personal data outside the context of the particular transaction recognisable by data subject. This is a functional description, but, as recognised earlier, it should cover:

- All entities offering services in the non-trading platform business model (eg online advertising);
- Entities collecting personal data from public or private sources and offering them on the wholesale market (data brokers, data resellers);
- All other entities collecting personal data by tracking (online and offline) behaviour of data subjects;
- Entities profiling[1165] data subjects.

In this way, the stricter regulation would be bound to using personal data (or intention to use them) in a way which may breach informational autonomy. The exact scope of the regulation is, of course, an element of any particular policy. For example, some particularly sensitive types of data (eg health data) may be covered irrespective of the way they are used. However, it seems a good idea to have the system based on PMM open for other applications, because other new technologies which may suffer from purpose limitation principle (eg Internet of Things) could be willing to implement PMM.

[1164] This is because many small enterprises seem not to follow the rules, Annex 8 to European Commission ((SEC(2012) 72 final) 2012, p.131.

[1165] Definition in GDPR, Article 4(4).

(b) Restrictions on Personal Information Administrators and their activities

There is also a need for some restrictions to PIAs' activities to protect the fiduciary character of the relationship they have with data subjects. This means that PIA should be a fiduciary, specifically obliged to a higher than ordinary standard of care in respect of the interest of the data subject. To make this possible it may be necessary to legally separate PIA from benefitting from personal data it should handle. For example, PIAs should not receive any benefits either directly from service providers or from downstream data users. Also, it may be reasonable to impose further restrictions on their organisational relationships to service providers or even direct or indirect ownership (or personal dependency). All of these elements should be secured on the level of legal requirements and monitored by DPAs.

4. *Restrictions on binding up services with blanket consent*

A slightly different type of restriction should be related to service providers, who should not bind the service provision with processing of data unnecessary for such provision. It is hard to anticipate the problems posed by service providers in respect of introducing PMM, as they, as noted in Chapter IV, may benefit from this concept. However, a couple of topics appeared repeatedly in discussion during the author's first public presentations of the model. There seems to be a concern that service providers simply present users with 'take it or leave it' choice in which they would demand an individual policy for all data types and data uses possible to provide a service. The remedy for this, as noted in Chapter IV, is the prohibition of binding up provision of a service with processing of unnecessary data. Such a provision should secure the element of choice and be enough to prevent those problems.

Also, it may potentially happen that some service providers see in PMM only a threat for their revenue and would set an alternative pricing system for services applicable when data subjects' policies prevent more invasive data uses. In this way, they would implement an economic nudge to make users agree to data collection. However, this scenario is not so dangerous because several aspects are different than in the situation without PMM. Firstly, currently data uses are hidden in T&Cs, and after introducing PMM they will be visible for data subjects. Service providers would need to communicate to their customers that they want to use personal data in a particular way, for example, that they want to sell them without anonymisation to

third parties. This sets out the problem and intentions of such a service provider more clearly. The price given for such data use is clearly seen as a price for that particular use of data to which PIAs may provide an appropriate professional opinion.

Secondly, if a price (in money) is to be set for the services of service provider, this price will be normally assessed according to the rules of competition law. That is, in a case in which a service provider has market dominance, such a price should not be excessive[1166] and discriminative.[1167] Taking into account that the quarterly revenue per user (ARPU) of the largest service providers is on the level of dollars or tenths of dollars,[1168] this could indicate that paying a few dollars monthly for, for example, a social network service with privacy could be a viable option for data subjects and service providers. Where there is no dominant player on a given market, the price should not be a problem, because market competition could regulate price with the help of data portability.

[1166] In Europe Article 102 of TFEU. Eg Case C-27/76 *United Brands Company v Commission* [1978] CJEU; but, not all jurisdictions know such a legal concept, eg in Australia competition law requires harm to competition, OECD (DAF/COMP(2011)18) 2012, p.197. Similarly in New Zealand, Commerce Act 1986, s 36.

[1167] Eg Case T-228/97 *Irish Sugar plc v Commission* [1999] CJEU; broader discussion in OECD (DAF/COMP(2016)15) 2016.

[1168] See Chapter III.

VIII Conclusion

The evolution of the Internet and transformation of the economy and other spheres of social interactions are happening very rapidly. The scale of the incursion into privacy resulting from these developments justifies regulatory intervention but there is currently a lack of suitable regulatory tools. This is because the privacy threat arising from pervasive data collection is peculiar and the old tools, such as consent for data processing, fail to work properly in this new context. This thesis offers a solution to this problem showing that technology is not intrinsically privacy-invasive and that effective regulation is possible.

The thesis starts with Part I exploring the problem of consent and privacy. First, it shifts the focus from a single procedural act of individual authorisation (consent) to exercising autonomy in a privacy process. This is crucial because online services are based on long-term contracts where data collection is continuous and individual decisions have to be taken with understanding of what data have been collected and how they are to be used. Second, it shows the activities and business models which pose a threat to informational autonomy and explains the nature of these problems. They are caused by the one-sided design of ICT architecture and asymmetries of information which shift the power balance towards online service providers.

Knowing where the problems lie, Part II proposes an effective response to them. This response relies on implementing the Privacy Management Model, a comprehensive tool which creates the capacity to exercise an autonomous choice with respect to the whole individual privacy process. The functions of PMM (organising, planning, controlling) allow individuals to manage their privacy processes. However, for this solution to be effective, the PMM functions have to be implemented in the market in a way which helps correct the power imbalance between the parties. This can be achieved by using the set of tools presented in Chapter V, including Personal Information Administrators. Furthermore, as the problems come from the architecture of the 'online world', the countermeasures also have to rely on architecture. This is why Chapter VI shows the technical tools necessary to build the 'windows into the souls' of online service providers. Finally, legal regulations described in Chapter VII enable and support all required functions of privacy management system. These laws include an overarching legal principle – the right to individual self-determination – which covers all the necessary functions of privacy management and serves as a fundamental legal freedom

anchoring all other laws. The lower-level laws deemphasise consent and implement PMM functions and PIA business model for activities recognised earlier as threatening informational autonomy.

So, the thesis has shown what an effective privacy management system for Internet services should look like. In such a system individuals have a fair chance to participate in a modern digital society and to manage the level of their exposure to the actions of others. Implementing this system in the market presupposes no radical changes to existing market business models nor data flows. It just provides an additional mechanism for privacy management by the means of technical interfaces which operates on top of existing systems of online service providers.

Imagine technology which respects individuals by recognising their own privacy preferences starting from the point of deciding whether to collect their personal data. Instead of providing data subjects with endless queries about consent and making them to scroll down every new privacy policy, the systems would recognise that, for example, they do not wish to be photographed for religious reasons and they want to restrict profiling and sharing of their identity and behavioural data because they are a part of minority (or minorities). Furthermore, individuals may move across their digital world or even a physical world full of different interconnected sensors (Internet of Things) knowing that technology providers respect their privacy, because the Personal Information Administrator of their choice verifies that. That PIA, chosen, for example, because it focuses on that particular minority and provides sensible advice for its members, acts as their personal agent ("defender") allowing the surrounding technology to be adjusted "on the fly" to their particular needs. They would not need to worry that a new phone could be eavesdropping on them or that their personal security could be compromised based on their online data (which could be dangerous in a country with an oppressive majority). This can be achieved.

However, achieving this requires different tools of regulation from what is currently on offer and many small changes on the way: cutting off third-party tracking, defining standards for data and data uses, designing technical interfaces to control data, and probably finding a number of business factors which PIAs could use to compete on the market. Adding to this complexity is the fact that data subjects are often unaware of data collection, 'data insensitive',

and that service providers have been working hard to introduce the belief that in the modern times privacy has to be forgone.

Implementing all of these measures may be seen as a daunting task. However, the further the information society develops, the more important it is to find effective ways of exercising individual autonomy. If people give up control over data which describe them in detail (or, as some authors say, constitute them), the power over themselves shifts to the actual data controllers and those who use their data. At the end of the day it is a game of power and influence and, currently in the information society, power is concentrated in the hands of data holders. So, there is a need for a 'data Enlightenment' and a separation of powers.

This thesis can be seen as proposal for such a separation of powers. The undivided (so far) power of those who hold data and use them (service providers) should be split. This thesis shows that a significant part of this power should go to those who represent the individuals and help them to set the rules about their data and to control those rules (PIAs). This also requires powerful agencies to verify that all the rules in the system are respected (DPAs). This thesis presents a complete solution which gives some hope for overcoming the difficult problem of autonomy. The sooner decision-makers start solving this problem, develop this package of ideas and implement them, the more 'data conscious' and 'data sensitive' people will be.

Bibliography

A Cases

1. *Australia*

Duffy v Google Inc [2015] SASC 170.

2. *Canada*

A.T. v Globe24h.com 2017 FC 114.

Beals v Saldanha 2003 SCC 72.

Eldridge v British Columbia (Attorney General) (1997) 3 SCR 624 (SC).

Google Inc. v Equustek Solutions Inc 2017 SCC 34.

Lawson v Accusearch Inc. 2007 FC 125.

Libman v The Queen (1985) 2 SCR 178 (SC).

Morguard Investments Ltd. v De Savoye (1990) 3 SCR 1077 (SC).

RWDSU v Dolphin Delivery Ltd. (1986) 2 SCR 573 (SC).

Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers 2004 SCC 45.

3. *Council of Europe*

Amann v Switzerland (2000) 30 EHRR 843 (Grand Chamber, ECHR).

Evans v The United Kingdom (2007) 43 EHRR 21 (Grand Chamber, ECHR).

Flinkkilä and Others v Finland (25576/04) Section IV, ECHR 6 July 2010.

Leander v Sweden (1987) 9 EHRR 433 (ECHR).

Malone v The United Kingdom (1984) 7 EHRR 14 (ECHR).

Odièvre v France (2004) 38 EHRR 43 (Grand Chamber, ECHR).

PG and JH v The United Kingdom (2008) 46 EHRR 51 (Section III, ECHR).

Pretty v The United Kingdom (2002) 35 EHRR 1 (Section IV, ECHR).

Reklos and Davourlis v Greece (1234/05) Section I, ECHR 15 January 2009

Rotaru v Romania (28341/95) Grand Chamber, ECHR 4 May 2000.

Sciacca v Italy (2006) 43 EHRR 20 (Section IV, ECHR).

Uzun v Germany (2012) 54 EHRR 121 (Section V, ECHR).

Verlagsgruppe News GmbH and Bobi v Austria (59631/09) Section I, ECHR 4 March 2013.

Von Hannover v Germany (2005) 40 EHRR 1 (Section III, ECHR)

Von Hannover v Germany (No 2) (2012) 55 EHRR 15 (Grand Chamber, ECHR).

4. *European Union*

Case C-293/12 *Digital Rights Ireland Ltd v Ireland* [2015] QB 127 (CJEU)

Cruz Villalón Pedro *Opinion of Advocate General Cruz Villalón to the case C‑293/12 (Digital Rights Ireland)* (2013).

Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)* [2014] 1 QB 1022 (CJEU)

Case C-11/70 *Internationale Handelsgesellschaft v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970] ECR 1125.

Case T-228/97 *Irish Sugar plc v Commission of the European Communities* [1999] ECR II-2969.

Case C-411/10 *N.S. v Secretary of State for the Home Department* [2013] QB 102 (CJEU).

Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof v Osterreichischer Rundfunk* [2003] ECR I-4989.

Case CJEU C‑212/13, *František Ryneš v Úřad pro ochranu osobních údajů (Office for Personal Data Protection)* [2015] WLR 2607 (CJEU).

Case C-92/09, C‑93/09 *Schecke, Eifert v Land Hessen* (CJEU 9 November 2010).

Eleanor VE Sharpston *Opinion of Advocate General Sharpston to the joined Cases C‑92/09 (Schecke) and C‑93/09 (Eifert)* (2010).

Case C‑362/14 *Maximillian Schrems v Data Protection Commissioner* [2016] QB 527 (CJEU).

Case C-291/12 *Schwarz v Stadt Bochum* [2013] WLR(D) 386 (CJEU).

Cases C‑203/15, C‑698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2017] QB 771 (CJEU).

Case C-27/76 *United Brands Company v Commission of the European Communities* [1978] ECR 207.

Case C‑419/14 *WebMindLicenses Kft v Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság (Hungarian National Tax and Customs Authority)* [2016] 4 WLR 50 (CJEU).

Case C-141/12 *YS v Minister voor Immigratie, Integratie en Asiel* [2015] WLR 609 (CJEU).

Case COMP/M7217 *Facebook / WhatsApp* European Commission, 10 March 2014.

Case COMP/M4731 *Google/ DoubleClick* European Commission, 11 March 2008.

Case COMP/40099 Disconnect, Inc *Complaint of Disconnect, Inc, Regarding Google's infringement of Article 102 TFEU through bundling into the Android platform and the related exclusion of competing privacy and security technology* (2015).

5. *Germany*

Census Act (Volkszählungsurteil) [1983] 65 BVerfGE 1 (BVerfG).
(Translation in Jürgen Bröhmer and Clauspeter Hill 60 Years German Basic Law (2010) 144 ff.)

North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) [2008] 120 BVerfGE 274 (BVerfG).
(Translation <http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007en.html>.)

Nuremberg Higher Regional Court [2013] 84 BVerfGE 192 (BVerfG).
(Translation <http://www.bverfg.de/e/rk20130717_1bvr316708en.html>.)

6. *New Zealand*

A v Google New Zealand Ltd [2012] NZHC 2352.

Allistair Patrick Brooker v The Police [2007] NZSC 30.

Hosking v Runting [2004] NZCA 34.

7. *The United Kingdom*

Malone v Commissioner of Police of the Metropolis (No 2) [1979] Ch 344.

Titchener v British Railways Board [1983] UKHL 10.

B Legislation and International Instruments

1. *Australia*

Privacy Act 1988 (Cth).

2. *Canada*

Personal Information Protection and Electronic Documents Act 2000.

3. *Council of Europe*

The Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, signed 4 November 1950)

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108 (Strasbourg, signed 28 January 1981).

Parliamentary Assembly of the Council of Europe *Resolution 1165* (1998).

4. *European Union*

Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) 2002 (OJ L108/51).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July October 1995 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L201/37).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (OJ L281/31).

European Parliament resolution of 27 November 2014 on supporting consumer rights in the digital single market 2014/2973(RSP).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L119/1).

5. *OECD*

OECD *Guidelines governing the protection of privacy and transborder flows of personal data* (1980).

OECD *Guidelines governing the protection of privacy and transborder flows of personal data* (2013).

6. *New Zealand*

Fair Trading Act 1986.

Privacy Act 1993.

Telecommunications Act 2001.

C Books and Chapters

George J Agich *Autonomy and long-term care* (OUP, New York, 1993).

Marion Albers "Realizing the Complexity of Data Protection" in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds) *Reloading Data Protection* (Springer, 2014) 213.

Robert Alexy *A theory of constitutional rights* (OUP, New York, 2010).

Julia Angwin *Dragnet Nation* (reprint ed, St. Martin's Griffin, 2015).

Pauline Anthonysamy, Phil Greenwood and Awais Rashid "A Method for Analysing Traceability between Privacy Policies and Privacy Controls of Online Social Networks" in Bart Preneel and Demosthenes Ikonomou (eds) *Privacy Technologies and Policy* (Springer, 2012) 187.

Robert M Axelrod *The evolution of cooperation* (Basic Books, New York, 1984).

Robert Baldwin, Martin Cave and Martin Lodge *Understanding regulation* (2nd ed, OUP, New York, 2012).

Kenneth A Bamberger and Deirdre K Mulligan *Privacy on the ground* (The MIT Press, Cambridge, 2015).

Jonathan Barnes "Data protection: breach of statutory duty" in *The law of privacy and the media* (3rd ed, OUP, Oxford, 2016) 301.

Tom L Beauchamp and James F Childress *Principles of biomedical ethics* (7th ed, OUP, New York, 2013).

Stanley I Benn "Privacy, freedom, and respect for persons" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Colin J Bennett "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats" in *Managing Privacy Through Accountability* (Palgrave Macmillan, 2012) 33.

Colin J Bennett and Charles D Raab *The governance of privacy* (2nd ed, MIT Press, Cambridge, 2006).

Paul Bernal *Internet Privacy Rights* (Cambridge University Press, Cambridge, 2014).

Edward J Bloustein "Privacy as an aspect of human dignity: An answer to Dean Prosser" in *Individual & Group Privacy* (2nd ed, Transaction Publishers, New Brunswick, 2003) 186.

Carine Bournez and Claudio A Ardagna "Policy Requirements and State of the Art" in *Privacy and identity management for life* (Springer, 2011) 295.

Herbert Burkert "Privacy-Data Protection" in *Governance of Global Networks in the Light of Different Local Values* (Nomos, Badan-Baden, 2000) 43.

John Braithwaite *Regulatory capitalism* (Edward Elgar, Cheltenham, 2008).

John Braithwaite "Types of responsiveness" in *Regulatory theory: foundations and applications* (2017).

Jürgen Bröhmer and Clauspeter Hill *60 Years German Basic Law* (2010).

Roger Brownsword *Contract law* (2nd ed, OUP, New York, 2006).

Roger Brownsword "So What Does the World Need Now?" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland 2008).

Roger Brownsword "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer, Netherlands, 2009) 83.

Roger Brownsword and Karen Yeung (eds) *Regulating technologies* (Hart, Oxford;Portland, 2008).

Johannes A Buchmann (ed) *Internet Privacy: Options for adequate realisation* (Springer, Berlin, Heidelberg, 2013).

Sarah Buss "Personal Autonomy" in Edward N Zalta (ed) *The Stanford Encyclopedia of Philosophy* (winter 2016 ed, Stanford University, 2016).

Denis Butin and Daniel Le Métayer "Log Analysis for Data Protection Accountability" in *FM 2014: Formal Methods* (Springer, Cham, 2014) 163.

Andrew S Butler *The New Zealand Bill of Rights Act* (2nd ed, LexisNexis, Wellington, 2015).

Lee A Bygrave *Data privacy law* (OUP, Oxford, 2014).

Lee A Bygrave and Dag Wiese Schartum "Consent, Proportionality and Collective Power" in Serge Gutwirth and others (eds) *Reinventing Data Protection?* (Springer Netherlands, 2009).

Jan Camenisch, Simone Fischer-Hübner and Kai Rannenberg *Privacy and identity management for life* (Springer, 2011).

JC Cannon *Privacy in Technology* (International Association of Privacy Professionals, 2014).

Peter Carey *Data protection* (4th ed, OUP, Oxford, 2015).

Johann Čas "Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions" in Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds) *Computers, Privacy and Data Protection: an Element of Choice* (Springer, Netherlands, 2011) 139.

Fred H Cate "The Failure of Fair Information Practice Principles" in Jane K Winn (ed) *Consumer Protection in the Age of the "Information Economy"* (Ashgate Pub., Farnham, 2007) 341.

Lennon YC Chang and Peter Grabosky "The governance of cyberspace" in *Regulatory theory: foundations and applications* (2017) 533.

Julie E Cohen *Configuring the networked self* (2012).

Committee on Data Protection *Report of the Committee on Data Protection* (HM Stationery Office, 1978).

Committee on Privacy, Home Office *Report ('Younger report')* (HM Stationery Office, London, 1972).

Chris Connolly and Peter van Dijk "Enforcement and Reform of the EU-US Safe Harbor Agreement" in David Wright and Paul De Hert (eds) *Enforcing Privacy* (Springer, 2016) 261.

Paul De Hert and Serge Gutwirth "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action" in Yves Poullet, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer, Netherlands, 2009) 3.

Judith Wagner DeCew *In pursuit of privacy* (Cornell University Press, Ithaca, 1997).

Pedro Domingos *The master algorithm* (Basic Books, New York, 2015).

Peter Drahos *Regulatory theory* (2017).

Peter Drahos and Martin Krygier "Regulation, institutions and networks" in *Regulatory theory: foundations and applications* (2017) 1.

Gerald Dworkin *The theory and practice of autonomy* (Cambridge University Press, Cambridge, 1988).

Dave Eggers *The Circle* (Vintage Books, New York, 2014).

David S Evans and Richard Schmalensee *Matchmakers* (Harvard Business Review Press, 2016).

Ariel Ezrachi and Maurice E Stucke *Virtual competition* (Harvard University Press, Cambridge, 2016).

Ruth R Faden and Tom L Beauchamp *A history and theory of informed consent* (OUP, New York, 1986).

Michelle Finneran Dennedy, Jonathan Fox and Thomas R Finneran *The Privacy Engineer's Manifesto* (Apress, Berkeley, 2014).

David H Flaherty *Protecting privacy in surveillance societies* (University of North Carolina Press, Chapel Hill, 1989).

Luciano Floridi *Information* (OUP, 2010).

Luciano Floridi *The fourth revolution* (OUP, New York, 2014).

Michel Foucault *Discipline and punish* (2nd ed, Vintage Books, New York, 1995).

Michel Foucault *Power* (New Press, New York, 2000).

Susy Frankel and John Yeabsley "Learning from the past, adapting for the future: regulatory reform in New Zealand" in Susy Frankel (ed) *Learning from the past, adapting for the future: regulatory reform in New Zealand* (LexisNexis, Wellington, 2011).

Arie Freiberg *The tools of regulation* (Federation Press, 2010).

Charles Fried "Privacy [a moral analysis]" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Francis Fukuyama *Trust* (Free Press, New York, 1995).

Ruth Gavison "Privacy and the limits of law" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Robert Gellman and Pam Dixon "Failures of Privacy Self-Regulation in the United States" in David Wright and Paul De Hert (eds) *Enforcing Privacy* (Springer, 2016) 53.

Rebecca Giblin *Code wars* (Edward Elgar Publishing, 2011).

Jennifer Golbeck (ed) *Computing with Social Trust* (Springer, London, 2009).

Jack L Goldsmith and Tim Wu *Who controls the Internet?* (OUP, New York, 2006).

Abraham S Goldstein "Legal Control of the Dossier" in *On Record: Files and Dossiers in American Life* (Russell Sage, 1969) 449.

Inge Graef *EU competition law, data protection and online platforms* (Kluwer Law, The Netherlands, 2016).

Neil Gunningham, Peter N Grabosky and Darren Sinclair *Smart regulation* (Clarendon Press, Oxford, 1998).

Neil Gunningham and Darren Sinclair "Smart Regulation" in (2017) in *Regulatory theory: foundations and applications* (2017) 133.

Serge Gutwirth, Paul De Hert and Laurent De Sutter "The Trouble with Technology Regulation: Why Lessig's 'Optimal Mix' Will Not Work" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Serge Gutwirth and Mireille Hildebrandt "Some Caveats on Profiling" in Serge Gutwirth, Yves Poullet and Paul De Hert (eds) *Data Protection in a Profiled World* (Springer, Netherlands, 2010) 31.

Kai He, Jian Weng, Joseph K Liu, Wanlei Zhou and Jia-Nan Liu "Efficient Fine-Grained Access Control for Secure Personal Health Records in Cloud Computing" in *Network and System Security* (Springer, Cham, 2016) 65.

Jonathan Herring *Medical law and ethics* (5th ed, OUP, Oxford, 2014).

Mireille Hildebrandt "A Vision of Ambient Law" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland 2008).

Robert A Hillman (ed) "Online boilerplate" in *Boilerplate: the foundation of market contracts* (Cambridge University Press, New York, 2007) 83.

M Hilty, A Pretschner, D Basin, C Schaefer and T Walter "A Policy Language for Distributed Usage Control" in *Computer Security – ESORICS 2007* (Springer, Berlin, Heidelberg, 2007) 531.

Leif-Erik Holz, Harald Zwingelberg and Marit Hansen "Privacy Policy Icons" in *Privacy and identity management for life* (Springer, 2011) 279.

Chris Jay Hoofnagle *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press, Cambridge, 2016).

Christopher C Hood and Helen Z Margetts *The Tools of Government in the Digital Age* (Palgrave Macmillan, Basingstoke, 2007).

Peter Hustinx "EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation" Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law (2013), forthcoming in in Marise Cremona (ed) *New Technologies and EU Law* (OUP, 2017).

Julie C Inness *Privacy, Intimacy, and Isolation* (OUP, 1996).

Bart Jacobs "Architecture Is Politics: Security and Privacy Issues in Transport and Beyond" in Serge Gutwirth, Yves Poullet and Paul De Hert (eds) *Data Protection in a Profiled World* (Springer, Netherlands, 2010) 289.

Xiaodong Jiang, Jason I Hong and James A Landay "Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing" in Gaetano Borriello and Lars Erik Holmquist (eds) *UbiComp 2002: Ubiquitous Computing* (Springer, Berlin; Heidelberg, 2002) 176.

Meg Leta Jones *Ctrl + Z* (New York University Press, New York, 2016).

Günter Karjoth, Matthias Schunter and Michael Waidner "Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data" in *Privacy Enhancing Technologies* (Springer, Berlin; Heidelberg, 2002) 69.

Nancy S Kim *Wrap Contracts* (Oxford Scholarship Online, 2013).

Michael Kirby "New Frontier: Regulating Technology by Law and 'Code'" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

John Kleinig "The Nature of Consent" in *The Ethics of Consent: Theory and Practice* (Oxford Scholarship Online, 2010).

Bert-Jaap Koops "Criteria for Normative Technology: The Acceptability of 'Code as law' in Light of Democratic and Constitutional Values" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Eleni Kosta *Consent in European Data Protection Law* (Martinus Nijhoff, Leiden, 2013).

Gina Kounga and Liqun Chen "Enforcing Sticky Policies with TPM and Virtualization" in *Trusted Systems* (Springer, Berlin; Heidelberg, 2011) 32.

Herke Kranenborg "Article 8" in *The EU Charter of Fundamental Rights: A Commentary* (Bloomsbury Publishing, 2014) 223.

Ronald J Krotoszynski, Jr *Privacy Revisited* (OUP, 2016).

Graeme Laurie *Genetic privacy* (Cambridge University Press, Cambridge, 2002).

Daniel Le Métayer "Whom to Trust? Using Technology to Enforce Privacy" in David Wright and Paul De Hert (eds) *Enforcing Privacy* (Springer, 2016) 395.

Lawrence Lessig *Code* (Basic Books, New York, 2000).

Lawrence Lessig *Code* (2nd ed, Basic Books, New York, 2006).

Rick Levine, Christopher Locke, Doc Searls and David Weinberger *The cluetrain manifesto* (ft.com, London, 2000).

Miriam Lips and Barbara Löfgren *Kiwis Managing their Online Identity Information* (VUW, Wellington, 2015).

Christoph Mallmann *Datenschutz in Verwaltungs-Informationssystemen (Data protection in information system administration)* (Oldenbourg Verlag, München, Wien, 1976).

Gary T Marx *Windows into the soul* (The University of Chicago Press, Chicago, 2016).

Victor Mayer-Schönberger "Generational development of data protection in Europe" in *Technology and Privacy : The New Landscape* (The MIT Press, Cambridge, 1997) 219.

Viktor Mayer-Schönberger and Kenneth Cukier *Big data* (Murray, London, 2013).

John S Mbiti *African religions & philosophy* (Heinemann, London; Ibadan, 1969).

TJ McIntyre and Colin Scott "Internet Filtering: Rhetoric, Accountability and Responsibility" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Colin HH McNairn *A guide to the Personal Information Protection and Electronic Documents Act* (LexisNexis, Ohio, 2007).

John Stuart Mill *On Liberty* (Cambridge University Press, Cambridge, 1859).

Arthur Raphael Miller *The assault on privacy* (University of Michigan Press, Ann Arbor, 1971).

William J Mitchell *City of bits* (MIT Press, Cambridge, 1995).

Adam D Moore *Privacy rights moral and legal foundations* (Pennsylvania State Univ. Press, 2010).

Nicole Moreham, Mark Warby, Michael Tugendhat and Iain Christie (eds) *The law of privacy and the media* (3rd ed, OUP, Oxford, 2016).

Bronwen Morgan and Karen Yeung *An Introduction to Law and Regulation* (2007).

Karen Mossberger, Caroline J Tolbert and Mary Stansbury *Virtual Inequality* (Georgetown University Press, 2003).

Andrew D Murray "Conceptualising the Post-Regulatory (Cyber)state" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Neil C Manson and Onora O'Neill *Rethinking informed consent in bioethics* (Cambridge University Press, Cambridge, 2007).

Helen Nissenbaum *Privacy in Context* (Stanford University Press, 2009).

OECD (ed) *Online identity theft* (OECD, Paris, 2009).

Anthony I Ogus *Regulation* (Hart Publishing, Oxford, 2004).

Onora O'Neill *Autonomy and trust in bioethics* (Cambridge University Press, Cambridge, 2002).

Alexander Novotny and Sarah Spiekermann "Personal information markets and privacy: A new model to solve the controversy" in Mirelle Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook 2013: The Value of Personal Data* (IOS Press, 2013) 102.

Eli Pariser *The Filter Bubble* (Penguin UK, 2011).

Siani Pearson "Privacy Management in Global Organisations" in Bart De Decker and David W Chadwick (eds) *Communications and Multimedia Security* (Springer, Berlin; Heidelberg, 2012) 217.

Stephen Penk and Rosemary Tobin *Privacy law in New Zealand*, Warren J. Brookbanks, Donna Maree Cross, David Harvey, William C. Hodge, Natalya King, Khylee Quince and Pauline Tapp (eds) (2nd ed, Thomson Reuters, Wellington, 2016).

Sandra Petronio *Balancing the Secrets of Private Disclosures* (Routledge, 1999).

Plato "Symposium" <http://classics.mit.edu/Plato/symposium.html>.

Robert D Putnam *Making democracy work* (Princeton University Press, Princeton, 1993).

Charles Raab "The Meaning of 'Accountability' in the Information Privacy Context" in Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds) *Managing Privacy through Accountability* (Palgrave Macmillan UK, 2012) 15.

Charles D Raab and Paul De Hert (eds) "Tools for Technology Regulation: Seeking Analytical Approaches" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Margaret Jane Radin (ed) "Boilerplate Today: The Rise of Modularity and the Waning of Consent" in *Boilerplate: the foundation of market contracts* (Cambridge University Press, New York, 2007) 189.

John Rawls *A theory of justice* (rev. ed, OUP, Oxford, 1999).

Joseph Raz *The Morality of Freedom* (Clarendon, Oxford, 1986).

Andrews Reath *Agency and autonomy in Kant's moral theory* (Clarendon, Oxford, 2006).

Jeffrey H Reiman "Privacy, intimacy, and personhood" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Neil M Richards *Intellectual privacy* (OUP, Oxford; New York, 2015).

Janice Richardson *Law and the philosophy of privacy* (Routledge, Abingdon, Oxon; New York, 2016).

Julian Rivers "A Theory of Constitutional Rights and the British Constitution" in *A theory of constitutional rights* (OUP, New York, 2010) xvii.

Stephen P Robbins, Rolf Bergman, Ian Stagg and Mary Coulter *Management* (7th ed, Pearson Australia, 2015).

Stefano Rodotà "Data Protection as a Fundamental Right" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer Netherlands, 2009) 77.

Arnold Roosendaal "We Are All Connected to Facebook … by Facebook!" in Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet (eds) *European Data Protection: In Good Health?* (Springer Netherlands, 2012) 3.

Antoinette Rouvroy and Yves Poullet "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer Netherlands, 2009) 45.

Diane Rowland, Uta Kohl and Andrew Charlesworth *Information technology law* (5th ed, Routledge, Abingdon, Oxon; New York, 2017).

Michael J Sandel *Liberalism and the Limits of Justice* (2nd ed, Cambridge University Press, Cambridge, 1998).

Michael J Sandel *What money can't buy* (Allen Lane, London; New York, 2012).

Sarah Spiekermann *Ethical IT Innovation* (Auerbach Publications, 2015).

Jerome B Schneewind *The invention of autonomy* (Cambridge University Press, Cambridge, 1998).

Bruce Schneier *Data and Goliath* (WWNorton & Company, New York, 2015).

Ferdinand Schoeman "Privacy and intimate information" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Colin Scott "Regulation in the Age of Governance: The Rise of the Post Regulatory State" in *The politics of regulation: institutions and regulatory reforms for the age of governance* (Edward Elgar, Cheltenham, 2005).

Doc Searls *The Intention Economy* (Harvard Business Review Press, Boston, 2012).

Secretary's Advisory Committee on Automated Personal Data Systems *Records, Computers, and the Rights of Citizens* (US Department of Health, Education & Welfare, 1973).

Nigel Shadbolt "Midata: Towards a personal information revolution" in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Forum Yearbook 2013: The Value of Personal Data* (IOS Press, 2013) 202.

Adam Shostack *Threat Modeling* (Wiley, Somerset, 2014).

Adam Smith *Wealth of nations* (BiblioBytes; NetLibrary, Hoboken, 1776).

Daniel J Solove *Understanding privacy* (Harvard University Press, Cambridge, 2008).

Aleksandr Solzhenitsyn *Cancer Ward (Раковый Корпус)* (Vintage Books, 2003).

Sarah Spiekermann *User control in ubiquitous computing* (Shaker, Aachen, 2008).

Maurice E Stucke and Allen P Grunes *Big data and competition policy* (OUP, Oxford, 2016).

Cass R Sunstein *After the rights revolution* (Harvard University Press, Cambridge, 1990).

Richard H Thaler and Cass R Sunstein *Nudge* (revised ed, Penguin Books, New York, 2009).

Michael J Trebilcock *The limits of freedom of contract* (Harvard University Press, Cambridge, 1993).

Markus Tschersich "Configuration Behavior of Restrictive Default Privacy Settings on Social Network Sites" in Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli and Neeraj Suri (eds) *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* (Springer, 2015) 77.

Sherry Turkle *Reclaiming conversation* (Penguin Press, New York, 2015).

Colin Turpin and Adam Tomkins *British government and the constitution* (6th ed, Cambridge University Press, Cambridge; New York, 2007).

Henk Van Rossum *Privacy-enhancing technologies* (Registratiekamer; Information and Privacy Commissioner/Ontario, Rijswick, The Netherlands; Toronto, Ont., Canada, 1995).

Jasper van de Ven and Frank Dylla "Qualitative Privacy Description Language" in *Privacy Technologies and Policy* (Springer, Cham, 2016) 171.

Raymond Wacks *Personal information* (Clarendon Press, Oxford, 1993).

Andreas Weigend *Data for the people* (Basic Books, New York, 2017).

Alan Westin "The origins of modern claims to privacy" in *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984).

Alan F Westin *Privacy and freedom* (Atheneum, New York, 1967).

Edgar A Whitley "Towards effective, consent based control of personal data" in Mirelle Hildebrandt, Kieron O'Hara and Michael Waidner (eds) *Digital Enlightenment Yearbook 2013: The Value of Personal Data* (IOS Press, 2013) 165.

Georg Henrik von Wright *The varieties of goodness* (Routledge & Kegan Paul, London, 1963).

Karen Yeung "Towards an Understanding of Regulation by Design" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

Gabriela Zanfir "Forgetting About Consent. Why The Focus Should Be On 'Suitable Safeguards' in Data Protection Law" in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds) *Reloading Data Protection* (Springer Netherlands, 2014) 237.

Jonathan Zittrain "Perfect Enforcement On Tomorrow's Internet" in *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart, Oxford; Portland, 2008).

D Journal Articles

Serge Abiteboul, Benjamin André and Daniel Kaplan "Managing your digital life" (2015) 58 Commun ACM 32.

Alessandro Acquisti and Christina M Fong "An Experiment in Hiring Discrimination Via Online Social Networks" (2014) SSRN.

Alessandro Acquisti, Allan Friedman and Rahul Telang "Is there a cost to privacy breaches? An event study" (2006) ICIS Proceedings 94.

Alessandro Acquisti and Jens Grossklags "Privacy and rationality in individual decision making" (2005) 3 IEEE Secur Priv 26.

Alessandro Acquisti, Curtis Taylor and Liad Wagman "The Economics of Privacy" (2016) 54 J Econ Lit 442.

Rakesh Agrawal and Christopher Johnson "Securing electronic health records without impeding the flow of information" (2007) 76 Int J Med Inform. 471.

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant and Yirong Xu "XPref: A preference language for P3P" (2005) 48 Computer Networks 809.

George A Akerlof "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism" (1970) 84 Q J Econ 488.

Joseph Alhadeff, Brendan van Alsenoy, and Jos Dumortier "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions" (2011) SSRN.

Anita L Allen "Coercing Privacy" (1999) 40 Wm & Mary L Rev 723.

Irwin Altman "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33 J Soc Issues 66.

Cédric Argenton and Jens Prüfer "Search engine competition with network externalities" (2012) 8 J Competition L & Econ 73.

M Armstrong "Competition in two-sided markets" (2006) 37 RJE 668.

Jane Bailey "Framed by Section 8: Constitutional Protection of Privacy in Canada" (2008) 50 Canadian J Criminology & Crim Just 279.

William Barnes, Myles Gartland and Martin Stack "Old Habits Die Hard: Path Dependency and Behavioral Lock-In" (2004) 38 J Econ Issues 371.

Jay B Barney and Mark H Hansen "Trustworthiness as a Source of Competitive Advantage" (1994) 15 Strategic Management J 175.

Solon Barocas and Andrew D Selbst "Big Data's Disparate Impact" (2016) 104 Cal L Rev 671.

Patricia Beatty, Ian Reay, Scott Dick and James Miller "P3P Adoption on E-Commerce Web sites: A Survey and Analysis" (2007) 11 IEEE Internet Comput 65.

Patricia Beatty, Ian Reay, Scott Dick and James Miller "Consumer Trust in e-Commerce Web Sites: A Meta-study" (2011) 43 ACM Comput Surv.

Moritz Y Becker, Alexander Malkis and Laurent Bussard "S4P: A generic language for specifying privacy preferences and policies" (2010) 167 Microsoft Research.

Ralf Bendrath "Privacy self-regulation and the changing role of the state: From public law to social and technical mechanisms of governance" (2007) EconStor.

Colin J Bennett "International Privacy Standards: Can Accountability be Adequate?" (2010) 106 Privacy Laws and Business International 21.

Colin J Bennett "In Defence of Privacy: The concept and the regime" (2011) 8 Surveill Soc 485.

Omri Ben-Shahar and Carl E Schneider "The Failure of Mandated Disclosure" (2011) 159 U Pa L Rev 647.

Marcin Betkier "Individual Privacy Management" (2016) 21 MALR 315.

Julia Black "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" (2001) 54 Curr Legal Probs 103.

Julia Black "Critical reflections on regulation" (2002) 27 Austl J Leg Phil 1.

Robert M Bond, Christopher J Fariss, Jason J Jones, Adam DI Kramer, Cameron Marlow, Jaime E Settle and James H Fowler "A 61-million-person experiment in social influence and political mobilization" (2012) 489 Nature 295.

William Bonner and Mike Chiasson "If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy" (2005) 15 Information and Organization 267.

danah boyd "Networked Privacy" (2012) 10 Surveill Soc 348.

Anu Bradford "The Brussels Effect" (2012) 107 Nw U L Rev 1.

Ian Brown "The Economics of Privacy, Data Protection and Surveillance" (2013) SSRN.

Paula J Bruening and K Krasnow Waterman "Data Tagging for New Information Governance Models" (2010) 8 IEEE Secur Priv 64.

Lee A Bygrave "The Place of Privacy in Data Protection Law Forum: Valuing Privacy: Legal Protections and Exceptions" (2001) 24 UNSWLJ 277.

Lee A Bygrave "Automated profiling: Minding the machine: Article 15 of the EC Data Protection Directive and automated profiling" (2001) 17 Comput Law Secur Rev 17.

Ryan Calo "The Boundaries of Privacy Harm" (2011) 86 Ind LJ 1131.

Ryan Calo "Digital Market Manipulation" (2014) 82 Geo Wash L Rev 995.

Joseph A Cannataci and Jeanne Pia Mifsud-Bonnici "Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty" (2005) 14 I&CTL 5.

Fred H Cate and Viktor Mayer-Schönberger "Notice and consent in a world of Big Data" (2013) 3 IDPL 67.

Ursula Cheer "The future of privacy: Recent legal developments in New Zealand" (2007) Canta LR 169.

Alex Chisholm and Nelson Jung "Platform regulation–ex-ante versus ex-post intervention: Evolving our antitrust tools and practices to meet the challenges of the digital economy" (2015) 11 Competition Policy International.

Galexia Chris Connolly "The US Safe Harbor-Fact or Fiction?" (2008) Galexia.

Julie E Cohen "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan L Rev 1373.

Anthony J Colangelo "What Is Extraterritorial Jurisdiction" (2014) 99 Cornell L Rev 1303.

Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M McDonald and Abdur Chowdhury "P3P deployment on websites" (2008) 7 Electronic Commer R A 274.

Mary J Culnan and Robert J Bies "Consumer Privacy: Balancing Economic and Justice Considerations" (2003) 59 J Soc Issues 323.

Bernhard Debatin, Jennette P Lovejoy, Ann-Kathrin Horn and Brittany N Hughes "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences" (2009) 15 J Comput Mediat Commun 83.

Detlev Zwick and Nikhilesh Dholakia "Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing" (2004) 24 J Macromarketing 31.

Claudia Diaz, Omer Tene and Seda Gürses "Hero or Villain: The Data Controller in Privacy Law and Technologies" (2013) 74 Ohio St LJ 923.

Frank H Easterbrook "Cyberspace and the Law of the Horse" (1996) 1996 U Chi Legal F 207.

Benjamin Edelman "Does Google leverage market power through tying and bundling?" (2015) 11 J Competition L & Econ 365.

Joseph Farrell "Can Privacy Be Just Another Good" (2012) 10 J Telecomm & High Tech L 251.

Simone Fischer-Hübner, Chris Jay Hoofnagle, Ioannis Krontiris, Kai Rannenberg, Michael Waidner and Caspar Bowden "Online Privacy – Towards Informational Self-Determination on the Internet" (2013) SSRN.

Dinei Florencio and Cormac Herley "Sex, Lies and Cyber-crime Surveys" (2011) Microsoft Research.

Luciano Floridi "The Ontological Interpretation of Informational Privacy" (2005) 7 Ethics Inf Technol 185.

Tamar Frankel "Trusting and non-trusting on the Internet" (2001) 81 B U L Rev 457.

Charles Fried "Privacy" (1968) 77 Yale LJ 475.

Maša Galič, Tjerk Timan and Bert-Jaap Koops "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation" (2017) 30 Philosophy & Technology 9.

Raphaël Gellert and Serge Gutwirth "The legal construction of privacy and data protection" (2013) 29 Comput Law Secur Rev 522.

Robert Gellman "Fair Information Practices: A Basic History" (2017) SSRN.

Rebecca Giblin "The P2P Wars: How Code Beat Law" (2012) 16 IEEE Internet Comput 92.

John Gilliom "A response to Bennett's 'In defence of privacy'" (2011) 8 Surveill Soc 500.

Robert Goff "Commercial contracts and the Commercial Court" (1984) LMCLQ 382.

H Tomas Gomez-Arostegui "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations" (2005) 35 Cal W Int LJ 153.

Inge Graef, Jeroen Verschakelen and Peggy Valcke "Putting the Right to Data Portability into a Competition Law Perspective" (2013) Law. The Journal of the Higher School of Economics Annual Review 53.

Graham Greenleaf "An endnote on regulating cyberspace: Architecture vs law?" (1998) 21 Univ of NSWLJ 593.

Graham Greenleaf "The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108" (2012) 2 IDPL 68.

Graham Greenleaf "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (2014) 23 JL Inf & Sci 4.

James Grimmelmann "Saving Facebook" (2009) 94 Iowa L Rev 1137.

Andres Guadamuz "Habeas Data vs the European Data Protection Directive" (2001) 3 JILT.

Gehan Gunasekara "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows" (2009) 17 Int J Law Info Tech 147.

Yuri Gurevich, Efim Hudis and Jeannette Wing "Inverse Privacy" (2014) Microsoft Research.

Kevin D Haggerty and Richard V Ericson "The surveillant assemblage" (2000) 51 Br J Sociol 605.

Andrei Hagiu and Bruno Jullien "Why do intermediaries divert search?" (2011) 42 RJE 337.

Garrett Hardin “The Tragedy of the Commons” (1968) 162 Science 1243.

Justus Haucap and Ulrich Heimeshoff “Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?” (2013) 11 Int Econ Econ Policy 49.

Chris Jay Hoofnagle “Denialists’ Deck of Cards: An Illustrated Taxonomy of Rhetoric Used to Frustrate Consumer Protection Efforts” (2007) SSRN.

Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good and Dietrich J Wambach “Behavioral Advertising: The Offer You Can’t Refuse” (2012) 6 Harv Law & Pol’y Rev 273.

Xiaodong Jiang and JA Landay “Modeling privacy control in context-aware systems” (2002) 1 IEEE Pervasive Computing 59.

Leslie K John, Alessandro Acquisti and George Loewenstein “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information” (2011) 37 J Consumer Res 858.

Sidney M Jourard “Some Psychological Aspects of Privacy” (1966) 31 L & CP 307.

Karine Barzilai-Nahon “Toward a theory of network gatekeeping: A framework for exploring information control” (2008) 59 J Am Soc Inf Sci Technol 1493.

Saffija Kasem-Madani and Michael Meier “Security and privacy policy languages: A survey, categorization and gap identification” (2015) arXiv preprint arXiv:151200201.

Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare and Karen Melham “Dynamic consent: A patient interface for twenty-first century research networks” (2015) 23 Eur J Hum Genet 141.

Pauline T Kim “Data-Driven Discrimination at Work” (2017) 48 WMLR 857.

Bert-Jaap Koops “The trouble with European data protection law” (2014) 4 IDPL 250.

Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tom Chokrevski and Maša Galič “A Typology of Privacy” (2016) SSRN.

Douwe Korff and Ian Brown “New Challenges to Data Protection - Final Report” (2010) SSRN.

Douwe Korff and Ian Brown “The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats & Implications” (2013) SSRN.

Aleksandra Korolova “Privacy Violations Using Microtargeted Ads: A Case Study” (2011) 3 Journal of Privacy and Confidentiality 27.

Michal Kosinski, David Stillwell and Thore Graepel “Private traits and attributes are predictable from digital records of human behavior” (2013) 110 PNAS 5802.

Michal Kosinski, Yilun Wang, Himabindu Lakkaraju and Jure Leskovec “Mining big data to extract patterns and predict real-life outcomes” (2016) 21 Psychol Methods 493.

Adam DI Kramer, Jamie E Guillory and Jeffrey T Hancock "Experimental evidence of massive-scale emotional contagion through social networks" (2014) 111 PNAS 8788.

Vineet Kumar "Making 'Freemium' Work" (2014) 92 HBR 27.

Christopher Kuner "Data Protection Law and International Jurisdiction on the Internet (Part I)" (2010) 18 Int'l JL & Info Tech 176.

Christopher Kuner, Fred H Cate, Christopher Millard, Dan Jerker B Svantesson and Orla Lynskey "When two worlds collide: The interface between competition law and data protection" (2014) 4 IDPL 247.

Kenneth C Laudon "Markets and Privacy" (1996) 39 Commun ACM 92.

Christophe Lazaro and Daniel Le Métayer "Control over personal data: True remedy or fairytale?" (2015) 12 SCRIPTed.

C Leng, H Yu, J Wang and J Huang "Securing personal health records in clouds by enforcing sticky policies" (2013) 11 Telkomnika 2200.

Lawrence Lessig "Reading the Constitution in Cyberspace" (1996) 45 Emory L J 869.

Lawrence Lessig "The Law of the Horse: What Cyber Law Might Teach" (1999) 113 Harv L Rev 501.

Lawrence Lessig "The Architecture of Privacy" (1999) 1 Vand J Ent L & Prac 56.

Ninghui Li, Ting Yu and A Anton "A semantics based approach to privacy languages" (2006) 21 Computer Systems Science and Engineering 339.

Timothy Libert "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites" (2015) International Journal of Communication.

Rebecca Lipman "Online Privacy and the Invisible Market for Our Data" (2016) 120 Penn State Law Review 777.

Giacomo Luchetta "Is the Google Platform a Two-Sided Market?" (2012) SSRN.

Viktor Mayer-Schonberger "Demystifying Lessig" (2008) 2008 Wis L Rev 713.

Aleecia M McDonald and Lorrie Faith Cranor "The Cost of Reading Privacy Policies" (2008) 4 ISJLP 543.

Armando Menéndez-Viso "Black and white transparency: Contradictions of a moral metaphor" (2009) 11 Ethics Inf Technol 155.

Marco Casassa Mont, Vaibhav Sharma and Siani Pearson "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services" (2003) HP Laboratories Technical Report HPL-2003-49.

Marco Casassa Mont, Vaibhav Sharma and Siani Pearson "EnCoRe: Dynamic consent, policy enforcement and accountable information sharing within and across organisations" (2012) HP Laboratories Technical Report HPL-2012-36.

Yves-Alexandre de Montjoye, Erez Shmueli, Samuel S Wang and Alex Sandy Pentland "openPDS: Protecting the Privacy of Metadata through SafeAnswers" (2014) 9 PLoS ONE e98790.

Adam Moore "Defining Privacy" (2008) 39 Journal of Social Philosophy 411.

Adam D Moore "Privacy" (2012) SSRN.

NA Moreham "Why Is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" (2008) SSRN.

Nicole Moreham "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 L Q Rev 628.

James P Nehf "Shopping for Privacy on the Internet" (2007) 41 J Consum Aff 351.

Helen Nissenbaum "Securing trust online: wisdom or oxymoron?" (2001) 81 Boston University Law Review 635.

Helen Nissenbaum "Privacy as Contextual Integrity" (2004) 79 Wash L Rev 119.

Helen Nissenbaum "A Contextual Approach to Privacy Online" (2011) 140 Daedalus 32.

Paul Ohm "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA Law Review 1701.

Lukasz Olejnik, Tran Minh-Dung and Claude Castelluccia "Selling off privacy at auction" (2013) HAL.

WA Parent "Privacy, Morality, and the Law" (1983) 12 Philos Public Aff 269.

Siani Pearson and Marco Casassa-Mont "Sticky Policies: An Approach for Managing Privacy across Multiple Parties" (2011) 44 Computer 60.

Scott R Peppet "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future" (2011) 105 Nw U L Rev 1153.

Sandra Petronio "Brief Status Report on Communication Privacy Management Theory" (2013) 13 J Fam Commun 6.

Andreas Pfitzmann and Marit Hansen "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management" (2010) Technische Universitat Dresden.

Michael E Porter "How competitive forces shape strategy" (1979) 57 HBR 137.

Michael E Porter "The Five Competitive Forces That Shape Strategy" (2008) 86 HBR 78.

Richard A Posner "The Right of Privacy" (1978) 12 Ga L Rev 393.

Jens Prufer and Christoph Schottmüller "Competing with Big Data" (2017) SSRN.

Joel R Reidenberg "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1998) 76 Tex L Rev 553.

J Lee Riccardi "The German Federal Data Protection Act of 1977: Protecting the right to privacy?" (1983) 6 BC Int'l & Comp L Rev 243.

Jean-Charles Rochet and Jean Tirole "Platform Competition in Two-Sided Markets" (2003) 1 J Eur Econ Assoc 990.

Bjoern Roeber, Olaf Rehse, Robert Knorrek and Benjamin Thomsen "Personal data: How context shapes consumers' data sharing with organizations from various sectors" (2015) 25 Electron Markets 95.

Beate Roessler and Dorota Mokrosińska "Privacy and social interaction" (2013) 39 J Philos Soc Crit 771.

Denise M Rousseau, Sim B Sitkin, Ronald S Burt and Colin Camerer "Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust" (1998) 23 Acad Manag Rev 393.

Ira S Rubinstein and Woodrow Hartzog "Anonymization and Risk" (2016) 91 Wa L Rev 703.

Pamela Samuelson "Privacy As Intellectual Property?" (2000) 52 Stanf L Rev 1125.

Bart W Schermer "The limits of privacy in automated profiling and data mining" (2011) 27 Comput Law Secur Rev 45.

Bart W Schermer, Bart Custers and Simone van der Hof "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection" (2014) 16 Ethics Inf Technol 171.

Bruce Schneier "Power in the Age of the Feudal Internet" (2013) 6 MIND-Multistakeholder Internet Dialog 60.

Paul M Schwartz "Privacy and Democracy in Cyberspace" (1999) 52 Vand L Rev 1607.

Paul M Schwartz "Internet Privacy and the State" (2000) 32 Conn L Rev 815.

Paul M Schwartz "Beyond Lessig's Code for Internet privacy: Cyberspace filters, privacy control, and fair information practices" (2000) 2000 Wis L Rev 743.

Paul M Schwartz "Property, Privacy, and Personal Data" (2004) 117 Harv L Rev 2056.

Paul M Schwartz and Daniel J Solove "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 NYU L Rev 1814.

Gregory Shaffer "The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice" (1999) 5 Eur L J 419.

Spiros Simitis "Reviewing Privacy In an Information Society" (1987) 135 U Pa L Rev 707.

Daniel J Solove "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477.

Daniel J Solove "I've Got Nothing to Hide and Other Misunderstandings of Privacy" (2007) 44 San Diego L Rev 745.

Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

Evelyne JB Sørensen "The post that wasn't: Facebook monitors everything users type and not publish" (2016) 32 Comput Law Secur Rev 146.

Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme and Kai-Lung Hui "The challenges of personal data markets and privacy" (2015) 25 Electron Markets 161.

Sarah Spiekermann and Alexander Novotny "A vision for global privacy bridges: Technical and legal measures for international data markets" (2015) 31 Comput Law Secur Rev 181.

Lior Jacob Strahilevitz "Toward a Positive Theory of Privacy Law" (2013) 126 Harv L Rev 2010.

Xiang Su, Jarkko Hyysalo, Mika Rautiainen, Jukka Riekki, Jaakko Sauvola, Altti Ilari Maarala, Harri Hirvonsalo, Pingjiang Li and Harri Honko "Privacy as a Service: Protecting the Individual in Healthcare Data Processing" (2016) 49 Computer 49.

Omer Tene and Jules Polonetsky "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Nw J Tech & Intell Prop 239.

Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24 NZULR 222.

Matteo Turilli and Luciano Floridi "The ethics of information transparency" (2009) 11 Ethics Inf Technol 105.

Jennifer M Urban and Chris Jay Hoofnagle "The Privacy Pragmatic as Privacy Vulnerable" (2014) SSRN.

R Polk Wagner "Information wants to be free: Intellectual property and the mythologies of control" (2003) Colum L Rev 995.

Ye Diana Wang and Henry H Emurian "An overview of online trust: Concepts, elements, and implications" (2005) 21 Comput Hum Behav 105.

Adam Warren and James Dearnley "Data protection legislation in the United Kingdom: From development to statute 1969-84" (2005) 8 iCS 238.

Samuel D Warren and Louis D Brandeis "Right to Privacy" (1890) 4 Harv L Rev 193.

Richman Wee, Mark Henaghan and Ingrid Winship "Ethics: Dynamic consent in the digital age of biology: online initiatives and regulatory considerations" (2013) 5 J Prim Health Care 341.

Daniel J Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Jay Sussman "Information Accountability" (2008) 51 Commun ACM 82.

Alan F Westin "Social and Political Dimensions of Privacy" (2003) 59 J Soc Issues 431.

James Q Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) 113 Yale LJ 1151.

Jan Whittington and Chris Jay Hoofnagle "Unpacking Privacy's Price" (2012) 90 NC L Rev 1327.

Karen Yeung "Government by publicity management: Sunlight or spin" (2005) 2 Public Law 360.

Karen Yeung "'Hypernudge': Big Data as a mode of regulation by design" (2017) 20 iCS 118.

Wu Youyou, Michal Kosinski and David Stillwell "Computer-based personality judgments are more accurate than those made by humans" (2015) PNAS 201418680.

Tal Zarsky "Mine your own business!: making the case for the implications of the data mining of personal information in the forum of public opinion" (2002) 5 Yale J L & Tech 1.

Jonathan Zittrain "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication Symposium: Cyberspace and Privacy: A New Legal Paradigm" (2000) 52 Stan L Rev 1201.

Jonathan Zittrain "The Fourth Quadrant" (2010) 78 Fordham L Rev 2767.

Shoshana Zuboff "Big other: Surveillance capitalism and the prospects of an information civilization" (2015) 30 J Inf Technol 75.

Frederik J Zuiderveen Borgesius "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation" (2016) 32 Comput Law Secur Rev 256.

Yanjun Zuo and Timothy O'Keefe "Post-release information privacy protection: A framework and next-generation privacy-enhanced operating system" (2007) 9 Inf Syst Front 451.

E Reports, Standards and Other Documents

Jagdish Prasad Achara *Unveiling and Controlling Online Tracking* (PhD Thesis, Université Grenoble-Alpes, 2016).

Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (US).

Asia Pacific Economic Cooperation *APEC privacy framework* (APEC Secretariat, Singapore, 2005).

Article 29 Working Party *Opinion 4/2007 on the concept of personal data* (WP 136 2007).

Article 29 Working Party *Opinion 3/2010 on the principle of accountability* (WP 173 2010).

Article 29 Working Party *Opinion 8/2010 on applicable law* (WP 179 2010).

Article 29 Working Party *Opinion 15/2011 on the definition of consent* (WP187 2011).

Article 29 Working Party *Opinion 04/2012 on Cookie Consent Exemption* (WP 194 2012).

Article 29 Working Party *Opinion 03/2013 on purpose limitation* (WP 203 2013).

Article 29 Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217 2014).

Article 29 Working Party *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)* (WP 247 2017).

Article 29 Working Party *Revised guidelines on the right to data portability* (WP 242 rev.01 2017).

Attorney-General's Department, Commonwealth of Australia *Identity crime and misuse in Australia 2016* (2016).

Australian Government, Productivity Commission *Data Availability and Use Inquiry Report: Overview & Recommendations* (82 2017).

Guillaume Brochot, Julianna Brunini, Franco Eisma, Rebecah Larsen and Daniel J Lewis *Study on Personal Data Stores* (2015).

Bundeskartellamt and Autorité de la concurrence *Competition Law and Data* (2016).

Cabinet Office *Better choices: better deals - consumers powering growth* (URN 11/749, 2011).

Cabinet Office *midata: Government response to consultation* (URN 12/1283, 2012).

CIFAS *Fraudscape report 2017* (2017).

Centre for Information Policy Leadership *Data Protection Accountability: The Essential Elements A Document for Discussion* (2009).

Centre for Information Policy Leadership and Hunton&Williams LLP *Ten steps to develop a multilayered privacy notice* (2006).

Conseil National du Numerique *Platform Neutrality: Building an open and sustainable digital environment* (2014).

Alissa Cooper "Report from the Internet Privacy Workshop, RFC 6462" Internet Architecture Board (2012) <http://tools.ietf.org/html/rfc6462>.

Convention *CHARTE 4360/00 - Draft Charter of Fundamental Rights of the European Union – Summary of amendments presented by the Praesidium* (2000).

Convention *CHARTE 4423/00 - Draft Charter of Fundamental Rights of the European Union – Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4422/00* (2000).

Council of Europe *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1980).

Giuseppe D'Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, Athena Bourka, European Union and European Network and Information Security Agency (ENISA) *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics* (2015).

Jan Dhont, María Verónica Pérez Asinari, Yves Poullet, Joel R Reidenberg and Lee A Bygrave *Safe harbour decision implementation study* (PRS/2003/A0-7002/E/27 2004).

Peter Druschel, Michael Backes and Rodica Tirtea *The right to be forgotten - between expectations and practice - ENISA* (2011).

European Commission *Impact assessment accompanying the document (proposal of General Data Protection Regulation)* (SEC(2012) 72 final 2012).

European Commission *Proposal for a Regulation on Privacy and Electronic Communications* (2017).

European Commission *Technical Analysis of the transposition of the Data Protection Directive in the Member States* (European Commission, 2003).

European Data Protection Supervisor *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy* (2014).

European Data Protection Supervisor *Report of workshop on Privacy, Consumers, Competition and Big Data* (2014).

European Data Protection Supervisor *EDPS Opinion on Personal Information Management Systems* (9/2016 2016).

European Data Protection Supervisor *EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)* (6/2017 2017).

Federal Trade Commission *Data Brokers: A Call for Transparency and Accountability* (2014).

Federal Trade Commission *Big Data: A Tool for Inclusion or Exclusion?* (2016).

Fondation Internet Nouvelle Generation *Plaquette MesInfos* (2013).

Fondation Internet Nouvelle Generation *MesInfors pilot study* (2015).

Lothar Fritsch *State of the Art of Privacy-enhancing Technology (PET) - Deliverable D21 of the PETweb project* (1013 2007).

Future of IDentity in the Information Society. *A Vision of Ambient Law* (FIDIS D7.9 2007).

House of Lords *Oral evidence from David Evans and Ariel Ezrachi before The Select Committee on the European Union* (2015).

House of Lords *Oral evidence from Daniel Gordon, Alex Chisholm, and Nelson Jung before The Select Committee on the European Union* (2015).

House of Lords *Oral evidence from Giovanni Buttarelli before The Select Committee on the European Union* (2015).

House of Lords *Oral evidence from Daniel Zimmer and Thomas Weck before The Select Committee on the European Union* (2015).

House of Lords, Select Committee on European Union *Online Platforms and the Digital Single Market* (HL Paper 129 2016).

House of Lords *Written evidence from Monoplkommission before The Select Committee on the European Union (OPL0046)* (2015).

House of Lords *Written evidence from Orla Lynskey before The Select Committee on the European Union (OPL0054)* (2015).

House of Lords *Written evidence from Competition and Markets Authority (OPL0055)* (2015).

Information Commissioner's Office *Data protection rights: What the public want and what the public want from Data Protection Authorities* (2015).

Interim Synthesis and OECD *Data-driven Innovation for Growth and Well-being*.

International Telecommunication Union *ICT Facts&Figures The world in 2016* (2016).

International Telecommunication Union *ITU-T Y.2011: General principles and general reference model for Next Generation Networks* (2004).

ISO/IEC *29100:2011(E) Information technology - Security techniques - Privacy framework* (2011).

ISO/IEC *27001:2013(E) Information technology — Security techniques — Information security management systems — Requirements* (2013).

ISO/IEC *29101:2013(E) Information technology - Security techniques - Privacy architecture framework* (2013).

Kleiner Perkins Caufield Byers "2016 Internet Trends Report" <http://www.kpcb.com/blog/2016-internet-trends-report>.

Kleiner Perkins Caufield Byers "2017 Internet Trends Report" <http://www.kpcb.com/internet-trends>.

Ronald Koorn, Herman van Gils, Joris ter Hart, Paul Overbeek and Raul Tellegen *Privacy-Enhancing Technologies White Paper for Decision-Makers* (2004).

Douwe Korff *Comparative summary of national laws - EC study on implementation of Data Protection Directive* (ETD/2001/B5-3001/A/49 2002).

Douwe Korff *New Challenges to Data Protection Study - Country Report: Germany* (A.4 2010).

Law Commission *Invasion of Privacy : Penalties and Remedies : Review of the Law of Privacy : Stage 3 (Issues Paper)* (NZLC IP14 2009).

Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy, Stage 4 (Issues Paper)* (NZLC IP17 2010).

Mark Lizar and David Turner (eds) Kantara Initiative *Consent Receipt Specification* (2017).

London Economics *Study on the economic benefits of privacy-enhancing technologies (PETs) - report to the European Commission* (2010).

META Group *Privacy Enhancing Technologies* (1.1 2005).

Ricardo Neisse, Ioannis Kounelis, Gary Steri and Igor Nai Fovino *Privacy in Mobile Devices and Web-Applications* (JRC103740 2016).

New Zealand Data Futures Forum "Harnessing the economic and social power of data" n.d. <https://www.nzdatafutures.org.nz/discussion-documents>.

New Zealand Ministry of Justice *Regulatory Impact Statement: Supplementary Government Response to the Review of Privacy Act 1993* (2014).

OECD *Abuse of Dominance and Monopolisation* (OCDE/GD(96)131 1996).

OECD *Making Privacy Notices Simple* (DSTI/ICCP/REG(2006)5 2006).

OECD *The Role of Digital Identity Management in the Internet Economy* (DSTI/ICCP/REG(2008)10 2009).

OECD *Excessive Prices* (DAF/COMP(2011)18 2012).

OECD *Exploring the Economics of Personal Data* (DSTI/ICCP/IE/REG(2011)2 2013).

OECD *The Role and Measurement of Quality in Competition Analysis* (DAF/COMP(2013)17 2013).

OECD *Price discrimination: background note by the Secretariat to the 126th Meeting of the Competition Committee* (DAF/COMP(2016)15 2016).

Orange and Loudhouse "The Future of Digital Trust: A European study on the nature of consumer trust and personal data" (February 2014) <http://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf>.

Mark Page, Christophe Firth, Colin Rand and AT Kearney *The Internet Value Chain* (2016).

Mark Page, Laurent Viviez, Christophe Firth and AT Kearney *Internet Value Chain Economics* (2010).

Parliament of Australia, Environment and Communications References Senate Committee *The adequacy of protections for the privacy of Australians online* (2011).

Antti Poikola, Kai Kuikkaniemi and Ossi Kuittinen *My Data* (Liikenne-ja viestintäministeriö, 2014).

Telefonica and Centre for Information Policy Leadership *Reframing data transparency* (2016).

The Advisory Council to Google on the Right to be Forgotten (2015).

The Boston Consulting Group *The Internet Economy in the G-20* (2012).

The Boston Consulting Group *The value of our digital identity* (2012).

The Federal Trade Commission *The "Sharing" Economy: Issues Facing Platforms, Participants & Regulators: A Federal Trade Commission Staff Report* (2016).

The German Monopolies Commission (Monopolkommission) *Competition policy: The challenge of digital markets* (68 2015).

The Norwegian Data Protection Authority (Datatilsynet) *The great data race* (2015).

The Norwegian Data Protection Authority (Datatilsynet) *It's getting personal* (2017).

The Norwegian Data Protection Authority (Datatilsynet) *Tracking in public spaces* (2017).

The White House *Big Data: Seizing opportunities, Preserving Values* (2014).

The White House *Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy* (2012).

TNS Opinion & Social *Data Protection - Special Eurobarometer 431* (DS-02-15-415-EN-N 2015).

Nicolai Van Gorp and Olga Batura *Challenges for Competition Policy in the Digitalised Economy* (IP/A/ECON/2014-12 2015).

W3C "P3P: The Platform for Privacy Preferences" (P3P, 20 November 2007) <https://www.w3.org/P3P/>.

W3C "Tracking Preference Expression (DNT)" (20 August 2015) <https://www.w3.org/TR/tracking-dnt/>.

W3C "Tracking Compliance and Scope" (26 April 2016) <https://www.w3.org/TR/tracking-compliance/>.

World Economic Forum and Bain & Company Inc *Personal Data: The Emergence of a New Asset Class* (2011).

World Economic Forum "Rethinking Personal Data: Strengthening Trust" World Economic Forum <https://www.weforum.org/reports/rethinking-personal-data-strengthening-trust/> (2012).

F Presentations and Conference Papers

Alessandro Acquisti "Privacy in Electronic Commerce and the Economics of Immediate Gratification" in *Proceedings of the 5th ACM Conference on Electronic Commerce* (2004) 21.

Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi and Robert C Miller "Smart Homes that Monitor Breathing and Heart Rate" (ACM Press, 2015) 837.

Marine Albarède, Renaud Francou, Daniel Kaplan and Fondation Internet Nouvelle Generation *MesInfos Explorer's Notebook* (2013).

Anette Alén-Savikko, Nomi Byström, Harri Hirvonsalo, Harri Honko, Antti Kallonen, Yki Kortesniemi, Kai Kuikkaniemi, Tuomas Paaso, Olli Pitkänen, Antti Poikola, Samuli Tuoriniemi, Sari Vainikainen and Jani Yli-Kantola *MyData Architecture - The Stack by HIIT* <http://hiit.github.io/mydata-stack/>.

Tim Berners-Lee "The original proposal of the WWW" (1989) <https://www.w3.org/History/1989/proposal.html>.

Marcin Betkier "Reclaiming personal data" (The APSN 5th International Conference, Auckland, 14 December 2016).

Denis Butin, Marcos Chicote and Daniel Le Métayer "Log design for accountability" in *Security and Privacy Workshops (SPW),* (IEEE, 2013) 1.

Ramón Cáceres, Landon Cox, Harold Lim, Amre Shakimov and Alexander Varshavsky "Virtual Individual Servers As Privacy-preserving Proxies for Mobile Devices" in *Proceedings of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds* (2009) 37.

Maciej Cegłowski "Deep-Fried Data" (Collections as Data: Stewardship and Use Models to Enhance Access, Washington, 27 September 2016).

Amir Chaudhry, Jon Crowcroft, Heidi Howard, Anil Madhavapeddy, Richard Mortier, Hamed Haddadi and Derek McAuley "Personal data: Thinking inside the box" in *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives* (2015).

Yulia Cherdantseva and Jeremy Hilton "A Reference Model of Information Assurance & Security" (IEEE, September 2013) 546.

Andy Christensen, Andrew Cunningham, Jerry Engelman, Charles Green, Charles Kawashima, Steve Kiger, Danil Prokhorov, Levasseur Tellis, Barbara Wendling and Frank Barickman "Key considerations in the development of driving automation systems" in *24th enhanced safety vehicles conference. Gothenburg, Sweden* (2015).

David D Clark "A Cloudy Crystal Ball -- Visions of the Future" (24th Internet Engineering Task Force, July 1992).

Julie E Cohen "Code and Law between Truth and Power - London School of Economics public lecture" (video, 11 March 2015) <http://www.lse.ac.uk/newsAndMedia/videoAndAudio/channels/publicLecturesAndEvents/player.aspx?id=2972>.

Concordia "Alexander Nix - The Power of Big Data and Psychographics" (video, 27 September 2016) <https://www.youtube.com/watch?v=n8Dd5aVXLCc>.

George Danezis and Seda Gürses "A critical review of 10 years of Privacy Technology" (12 August 2010).

Susan B Davidson, Sanjeev Khanna, Sudeepa Roy, Julia Stoyanovich, Val Tannen and Yi Chen "On Provenance and Privacy" in *Proceedings of the 14th International Conference on Database Theory* (ACM, 2011) 3.

Lilian Edwards "Code, Law and Privacy: Privacy Invading, Enhancing, or Neutral?" (AHRC Research Centre for Studies in Intellectual Property and Technology Law, July 2004).

Deborah Estrin "What happens when each patient becomes their own 'universe' of unique medical data?" TEDMED (video, April 2013) <http://www.tedmed.com/talks/show?id=17762>.

European Commission *Commission Communication on the protection of Individuals in relation to the processing of personal data in the Community and information security* (1990).

Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove and Christo Wilson "Measuring Price Discrimination and Steering on E-commerce Web Sites" in *Proceedings of the 2014 Conference on Internet Measurement Conference* (ACM, 2014) 305.

Maurice Herlihy and Mark Moir "Blockchains and the Logic of Accountability: Keynote Address" in *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science* (2016) 27.

Harri Honko "MyData Reference Architecture@Mydata2016" (Helsinki, 31 August 2016).

IAPP MultiMedia "Peter Watts: Burn the Data to the Ground" (video, 31 May 2014) <https://www.youtube.com/watch?v=gLihNlDhu_E>.

Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor and Robert W Reeder "A nutrition label for privacy" in *Proceedings of the 5th Symposium on Usable Privacy and Security* (ACM, 2009) 4.

Patrick Gage Kelley, Lucian Cesca, Joanna Bresee and Lorrie Faith Cranor "Standardizing privacy notices: An online study of the nutrition label approach" in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* (ACM, 2010) 1573.

Michael Kirby "Opening remarks" (The APSN 5th International Conference, Auckland, 14 December 2016).

Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen and Charalampos Papamanthou "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts" (IEEE, May 2016) 839.

Lucja Kot "Tracking Personal Data Use: Provenance and Trust." in *CIDR* (2015).

Ponnurangam Kumaraguru, L Cranor, Jorge Lobo and Seraphin Calo "A survey of privacy policy languages" in *Workshop on Usable IT Security Management (USM 07): Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM* (2007).

Jakub Mikians, László Gyarmati, Vijay Erramilli and Nikolaos Laoutaris "Detecting price and search discrimination on the Internet," (HotNets workshop, 29 October 2012).

Nicole Moreham and Marcin Betkier "Privacy. Why should we care?" (Victoria University of Wellington Spotlight Lecture Series, Wellington, 15 April 2016).

Cathy O'Neil "Weapons of Math Destruction" (video, 7 June 2015) <https://www.youtube.com/watch?v=gdCJYsKlX_Y>.

Onora O'Neill "A Question Of Trust" *BBC Reith Lectures* (podcast, 2002) <http://www.bbc.co.uk/radio4/reith2002/>.

Nick Papanikolaou and Siani Pearson "A Cross-Disciplinary Review of the Concept of Accountability" in *Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)* (May 2013).

Jaehong Park and Ravi Sandhu "Towards Usage Control Models: Beyond Traditional Access Control" in *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies* (2002) 57.

Nathaniel Popper "Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency" *The New York Times* (21 August 2017) <https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html>.

re:publica "re:Publica 2017 - Maciej Ceglowski: Notes from an Emergency" (video, Berlin, 16 May 2017) <https://www.youtube.com/watch?v=rSrLjb3k1II>.

Rula Sayaf, Dave Clarke and James B Rule "The other side of privacy: Surveillance in data control" (ACM, 2015) 184.

Yong Yuan, Feiyue Wang, Juanjuan Li and Rui Qin "A survey on real time bidding advertising" in *2014 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)* (October 2014) 418.

G Internet Resources and Newspaper Articles

Accenture "Building digital trust: The role of data ethics in the digital age" <https://www.accenture.com/us-en/insight-data-ethics> (2016).

Julia Angwin "Own a Vizio Smart TV? It's Watching You" *ProPublica* (9 November 2015) <http://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you>.

Julia Angwin, Terry Parris, Surya Mattu and ProPublica "Breaking the Black Box: What Facebook Knows About You" *ProPublica* (28 September 2016) <https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you>.

Emily Bater "Midata: Making comparison better" Gocompare.com <http://www.gocompare.com/money/midata/>.

Peter Baugh "'Techplomacy': Denmark's ambassador to Silicon Valley" *Politico* (20 July 2017) <http://www.politico.eu/article/denmark-silicon-valley-tech-ambassador-casper-klynge/>.

Bojana Bellamy and Markus Heyder "Empowering Individuals Beyond Consent" *IAPP* (2 July 2015) <https://privacyassociation.org/news/a/empowering-individuals-beyond-consent/>.

Rahul Bhatia "The inside story of Facebook's biggest setback" *The Guardian* (12 May 2016) <http://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg>.

"BitsaboutMe" <https://bitsabout.me/en/>.

"Cambridge Analytica" <https://cambridgeanalytica.org/>.

Noam Chomsky, Edward Snowden, Glenn Greenwald and Nuala O'Connor "A Conversation on Privacy" *The Intercept* (25 March 2016) <https://theintercept.com/a-conversation-about-privacy/>.

Amit Chowdhry "Facebook Says It Is Not Listening To Your Conversations For Ads Using Microphone Access" *Forbes* (7 June 2016) <http://www.forbes.com/sites/amitchowdhry/2016/06/07/facebook-audio-from-your-smartphone-microphone-is-not-being-used-for-ads/>.

Customer Commons "Customer Commons and User Submitted Terms" (27 October 2014) <http://customercommons.org/2014/10/27/customer-commons-and-user-submitted-terms/>.

Kate Cox "Why Is Google Blocking This Ad-Blocker On Chrome?" (18 January 2017) Consumerist <https://consumerist.com/2017/01/18/why-is-google-blocking-this-ad-blocker-on-chrome/>.

Data Futures Partnership "A Path to Social Licence: Guidelines for Trusted Data Use" (1 September 2017) <http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/>.

"Datum" <https://datum.network>.

Jeff Desjardins "Google and Facebook dominate digital advertising" (12 December 2016) *Business Insider* <http://www.businessinsider.com/google-and-facebook-dominate-digital-advertising-2016-12>.

Digital Advertising Alliance "WebChoices: Digital Advertising Alliance's Consumer Choice Tool for Web (Beta)" <http://optout.aboutads.info/>.

"Disconnect" <http://disconnect.me>.

Jamie Doward and Alice Gibbs "Did Cambridge Analytica influence the Brexit vote and the US election?" *The Guardian* (4 March 2017) <https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump>.

"e-Residency - e-Estonia" <https://e-estonia.com/component/e-residency/>.

William D Eggers, Rob Hamill and Abed Ali "Data as the new currency: government's role in facilitating the exchange" *DU Press* (24 July 2014) <https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-13/data-as-the-new-currency.html>.

European Commission "Antitrust: Commission sends Statement of Objections to Google on Android operating system and applications" (Press release IP/16/1492, 20 April 2016) <http://europa.eu/rapid/press-release_IP-16-1492_en.htm>.

European Commission "Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service" (Press release IP/17/1784, 27 June 2017) <http://europa.eu/rapid/press-release_IP-17-1784_en.htm>.

"Executive Order: Enhancing Public Safety in the Interior of the United States" The White House (25 January 2017) <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>.

Facebook "2017 Q3 Results - Earnings Call Slides" *Seeking Alpha* (3 November 2017) <https://seekingalpha.com/article/4120214-facebook-2017-q3-results-earnings-call-slides>.

Facebook "Advertising policies" <https://www.facebook.com/policies/ads/>.

"Facebook - Data Policy" <https://www.facebook.com/full_data_use_policy>.

Lawrence Freeborn "IDC Comment: MiData - Government-Driven Initiative Brings Customer Data Analytics to Current Account Switching" *Targeted News Service* (8 April 2015) <http://search.proquest.com/docview/1674053332/citation/BD3878866CBC49BEPQ/1>.

Fondation Internet Nouvelle Generation "MesInfos project" <http://mesinfos.fing.org/english/>.

Future of Privacy Forum "Companies that have implemented Do Not Track" All About DNT <https://allaboutdnt.com/companies/>.

Feliks Garcia "Man pleads guilty to iCloud celebrity nude leak" *The Independent* (27 September 2016) <http://www.independent.co.uk/news/people/icloud-celebrity-nude-leak-jennifer-lawrence-kate-upton-man-pleads-guilty-a7334031.html>.

Patricia Garner "Average revenue per user is an important growth driver" *Market Realist* (11 Febuary 2015) <http://marketrealist.com/2015/02/average-revenue-per-user-is-an-important-growth-driver/>.

Samuel Gibbs "Privacy fears over 'smart' Barbie that can listen to your kids" *The Guardian* (13 March 2015) <http://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel>.

Paul Gil "What Is Whaling? (Phishing Attack)" *Lifewire* (22 March 2017) <https://www.lifewire.com/what-is-whaling-2483605>.

Google "Updates: Privacy Policy – Privacy & Terms" (27 June 2017) <https://www.google.co.nz/intl/en/policies/privacy/archive/>.

Google "Alphabet's (GOOG) CEO Sundar Pichai On Q2 2017 Results - Earnings Call Transcript" *Seeking Alpha* (25 July 2017) <https://seekingalpha.com/article/4090041-alphabets-goog-ceo-sundar-pichai-q2-2017-results-earnings-call-transcript>.

Google "Advertising Policies Help" <https://support.google.com/adwordspolicy/topic/2996750?hl=en&ref_topic=1308156,>.

Google "Personal info & privacy" <https://myaccount.google.com/privacy>.

Google "Manage or delete your Location History - Google Account Help" <https://support.google.com/accounts/answer/3118687>.

Google "Privacy Policy – Privacy & Terms" <http://www.google.com/policies/privacy/>.

Inge Graef and Van Alsenoy "Data protection through the lens of competition law: Will Germany lead the way?" *Inforrm's Blog* (24 March 2016) <https://inforrm.wordpress.com/2016/03/24/data-protection-through-the-lens-of-competition-law-will-germany-lead-the-way-inge-graef-and-brendan-van-alsenoy/>.

Graham Hill "Four Fallacies of Vendor Relationship Management" CustomerThink (23 January 2009) <http://customerthink.com/four_fallacies_vendor_relationship_management/>.

Andy Greenberg "Apple's Latest Selling Point: How Little It Knows About You" *Wired* (6 August 2015) <https://www.wired.com/2015/06/apples-latest-selling-point-little-knows/>.

Luke Hayter "Lookalike modelling: The ad industry technique demystified" *The Guardian* (6 September 2013) <https://www.theguardian.com/media-network/media-network-blog/2013/sep/06/lookalike-modelling-advertising-demystified>.

Jessi Hempel "Inside Facebook's Ambitious Plan to Connect the Whole World" *Wired* (20 January 2016) <http://www.wired.com/2016/01/facebook-zuckerberg-internet-org/>.

Alex Hern "Samsung rejects concern over 'Orwellian' privacy policy" *The Guardian* (9 February 2015) <http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy>.

Alex Hern "Vibrator maker ordered to pay out C$4m for tracking users' sexual activity" *The Guardian* (14 March 2017) <https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits>.

Daniela Hernandez "The inside story of how Apple's new medical research platform was born" *Fusion* (17 March 2015) <http://fusion.net/the-inside-story-of-how-apples-new-medical-research-pla-1793846479>.

Chris Jay Hoofnagle "Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)" *Berkeley Law* <https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/>.

HM Treasury "Is your bank giving you the best deal? Find out using new online comparison tool" (26 March 2015) <https://www.gov.uk/government/news/is-your-bank-giving-you-the-best-deal-find-out-using-new-online-comparison-tool>.

"Intercom - Free Customer Intelligence Platform" <https://www.intercom.io/customer-intelligence>.

"International Association of Privacy Professionals" <https://iapp.org/>.

Bala Iyer, Mohan Subramaniam and U Srinivasa Rangan "The Next Battle in Antitrust Will Be About Whether One Company Knows Everything About You" *Harvard Business Review* (6 July 2017) <https://hbr.org/2017/07/the-next-battle-in-antitrust-will-be-about-whether-one-company-knows-everything-about-you>.

Jasper Jackson "Google and Facebook to take 71% of UK online ad revenue by 2020" *The Guardian* (15 December 2016) <https://www.theguardian.com/media/2016/dec/15/google-facebook-uk-online-ad-revenue>.

Rupert Jones "Switching banks: Click and collect a made-to-measure current account" *The Guardian* (28 March 2015) <https://www.theguardian.com/money/2015/mar/28/switching-banks-current-account-midata-gocompare>.

Damian Le Nouaille "Instagram is listening to you" *Medium* (25 August 2017) <https://medium.com/@damln/instagram-is-listening-to-you-97e8f2c53023>.

Sam Levin "Facebook to give Congress thousands of ads bought by Russians during election" *The Guardian* (21 September 2017) <https://www.theguardian.com/technology/2017/sep/21/facebook-adverts-congress-russia-trump-us-election>.

Yasha Levine "Al Gore says Silicon Valley is a 'stalker economy'" *Pando* (11 June 2014) <https://pando.com/2014/06/11/al-gore-says-silicon-valley-is-a-stalker-economy/>.

"Loon for all – Project Loon" <https://www.google.co.nz/loon/>.

Martin Lopatka “Are trackers the new backbone of the Web?” *Medium* (1 August 2017) <https://medium.com/firefox-context-graph/are-trackers-the-new-backbone-of-the-web-fb800435da15>.

Mary Madden “Public Perceptions of Privacy and Security in the Post-Snowden Era” *Pew Research Center* (12 November 2014) <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

Matt McKeon “The Evolution of Privacy on Facebook” <http://mattmckeon.com/facebook-privacy/>.

David Meyer “European Commission, experts uneasy over WP29 data portability interpretation” IAPP (25 April 2017) <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/>.

MyData “MyData” <https://mydatafi.wordpress.com/>.

MyData.org “Berlin Memorandum” <https://mydata.org/berlin-memorandum/>.

NAI: Network Advertising Initiative “Consumer Opt-out” <http://www.networkadvertising.org/choices/>.

Arvind Narayanan “There is no such thing as anonymous online tracking” (28 July 2011) *Stanford Law School* <https://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking>.

Dave Lee “Facebook fake news row: Mark Zuckerberg is a politician now” *BBC News* (19 November 2016) <http://www.bbc.com/news/technology-38036730>.

OASIS “OASIS Universal Business Language (UBL)” <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl >.

OECD “2016 Economy Ministerial Meeting – The Digital Economy: Innovation, Growth and Sociual Prosperity” <http://www.oecd.org/internet/ministerial/> (2016).

Office of the Australian Information Commissioner (OAIC) “Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner” <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison>.

Office of the Privacy Commissioner “Does the Privacy Act apply to agencies based overseas?” <https://privacy.org.nz/further-resources/knowledge-base/view/154> (as of 8 July 2017).

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia “Getting Accountability Right with a Privacy Management Program” (17 April 2012) <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.

“Open mHealth – Open Source Data Integration Tools” Open mHealth <http://www.openmhealth.org/>.

Oxford Dictionaries <https://en.oxforddictionaries.com/>.

Oxford Internet Institute “Computational Propaganda Worldwide: Executive Summary” <http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-worldwide-executive-summary/>.

P2P Foundation “Vendor Relationship Management” (28 January 2012) <http://wiki.p2pfoundation.net/Vendor_Relationship_Management>.

PageFair “2017 Adblock Report” (1 February 2017) PageFair <https://pagefair.com/blog/2017/adblockreport/>.

“pcamidata.co.uk” <https://www.pcamidata.co.uk/>.

“Project VRM” <https://cyber.harvard.edu/projectvrm/Main_Page>.

Project VRM “VRM Development Work” <https://cyber.harvard.edu/projectvrm/VRM_Development_Work>.

Katarzyna Szymielewicz “Jak w sieci stajemy się towarem? Komercyjny Internet od zaplecza” (1 May 2017) <https://panoptykon.org/wiadomosc/jak-w-sieci-stajemy-sie-towarem-komercyjny-internet-od-zaplecza>.

Dave Raggett “Machine Interpretable Privacy Policies -- A fresh take on P3P” (2010) <https://www.w3.org/2010/09/raggett-fresh-take-on-p3p/>.

Julia Fioretti “France fines Google over ‘right to be forgotten’” *Reuters* (25 March 2016) <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX>.

Adam Richardson “Using Customer Journey Maps to Improve Customer Experience” *Harvard Business Review* (15 November 2010) <https://hbr.org/2010/11/using-customer-journey-maps-to>.

Katie Rogers “Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too.” *The New York Times* (22 June 2016) <https://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html>.

Doc Searls “Beyond ad blocking — the biggest boycott in human history” (29 September 2015) *Doc Searls Weblog* <https://blogs.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/>.

Connor Simpson “Uber Busted for Intentionally Surging Prices” *The Atlantic* (26 February 2014) <https://www.theatlantic.com/technology/archive/2014/02/uber-busted-intentionally-surging-prices/358555/>.

George Slefo “Apple’s Move to Kill Cookies Brings Plea From Six Major Trade Associations” AdAge (14 September 2017) <http://adage.com/article/digital/apple-s-party-tracking-update-y/310462/>.

Olivia Solon “Facebook has 60 people working on how to read your mind” *The Guardian* (19 April 2017) <https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8>.

Daniel Solove “The Hulk Hogan Gawker Sex Video Case, Free Speech, and the Verdict’s Impact” *LinkedIn Pulse* (20 March 2016) <https://www.linkedin.com/pulse/hulk-hogan-gawker-sex-video-case-free-speech-verdicts-daniel-solove>.

StatCounter Global Stats “StatCounter Global Stats” <http://gs.statcounter.com/>.

Nick Statt “How Facebook is taking mind reading from sci-fi to reality” *The Verge* (20 April 2017) <https://www.theverge.com/2017/4/20/15375176/facebook-regina-dugan-interview-building-8-mind-reading-f8-2017>.

Chandra Steele “How to Get Google to Quit Tracking You” *PCMag* (20 April 2017) Australia.<http://au.pcmag.com/gps-mapping-products/47543/news/how-to-get-google-to-quit-tracking-you>

Nick Szabo “The Idea of Smart Contracts” (1997) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>.

Ben Tarnoff “Can Engineers Change Silicon Valley’s Political Agenda?” *The Nation* (17 May 2017) <https://www.thenation.com/article/can-engineers-change-silicon-valleys-political-agenda/>.

MG Siegler “Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003” TechCrunch (4 August 2010) <http://techcrunch.com/2010/08/04/schmidt-data/>.

“The Data Brokers: Selling your personal information” (24 August 2014) <http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/>.

Twitter “Do Not Track” Twitter Help Center <https://help.twitter.com/articles/20169453?lang=en>.

Dan Tynan “Acxiom exposed: A peek inside one of the world’s largest data brokers” (15 May 2013) ITworld <http://www.itworld.com/article/2710610/it-management/acxiom-exposed--a-peek-inside-one-of-the-world-s-largest-data-brokers.html>.

Jonathan Underhill “Merged Fairfax, NZME would have just 12% of NZ digital ad market dominated by Google, Facebook” *The National Business Review* (27 May 2016) <https://www.nbr.co.nz/article/merged-fairfax-nzme-would-have-just-12-nz-digital-ad-market-dominated-google-facebook-b>.

Danielle Wiener-Bronner “Equifax breach: How a hack became a public relations catastrophe” *CNNMoney* (12 September 2017) <http://money.cnn.com/2017/09/12/news/companies/equifax-pr-response/index.html>.

“Your Online Choices - AU” <http://www.youronlinechoices.com.au/>.

“Your Online Choices - EU” <http://www.youronlinechoices.com/>.

"Your Online Choices - NZ" <http://www.youronlinechoices.co.nz/>.

Maciej Zawadziński "What is Look-alike Modeling and How Does it Work?" *Clearcode* (15 February 2017) <http://clearcode.cc/2017/02/look-alike-modeling/>.

Zeljka Zorz "Ashley Madison users blackmailed again" *Help Net Security* (25 April 2017) <https://www.helpnetsecurity.com/2017/04/25/ashley-madison-blackmail/>.

Schedules

A Comparison of Early Privacy Principles and Recommendations

Table 6 Comparison of early privacy principles and recommendations

	'Principle' or other recommendation	**Younger Committee (UK, 1972)**	**FIPPs (US, 1973)** (principles)	**Lindop Committee (UK, 1978)** (principles)	**Council of Europe Convention 108 (1981)**	**OECD Privacy Guidelines (1980)**
0	What value is balanced with privacy?	Use of computers for business purposes (para.573);	Use of data for 'shared purposes' (p.40);	Handling data in pursuit of lawful interest of data user (P6);	Free flow of information between the peoples;	Fundamental value of the free flow of information;
General prerequisites						
1	Fairness and lawfulness	Not explicitly	Governance by procedures which afford the individual a right to participate in deciding what is collected and what is disclosed. Unless the law says otherwise;	Not explicitly;	Data "obtained and processed fairly and lawfully" – as a part of quality criterion (Article 5a);	Data should be obtained by lawful and fair means – named 'collection limitation' (s 7);
2	Data Protection Officer	Appointing "a responsible person" (para.624);	"One person immediately responsible for the system" (p.54);	-	-	-
3	Accountability	-	Enforcement by civil and criminal sanctions (p.50);	Data subjects should be able to verify compliance (P5);	-	Data controller "should be accountable" (s 14);
Risk minimisation and quality						
4	Security of data	The level of security planned in advance and should include precaution against deliberate abuse (para.596);	Emphasised as important;	Not as a principle but envisaged as an important part of the future Code of Conduct (para.21.22);	Appropriate level of security against loss, destruction, unauthorised access, alteration, dissemination (Article 7);	Security safeguards (s 11);
5	Data minimisation	Minimum necessary for the specified purpose (para.593)	-	Collection "no more than necessary for the purposes made known or authorised" (P4);	adequate, relevant and not excessive – as a part of quality (Article 5c);	-

		Time limit on retention (para.598)				
6	Separating identities from data	Should be used in statistics (para.594)	-	-	Data preserved in a form which permits identification no longer than required for the purpose, then may be anonymised (Article 5e);	-
7	Quality of data	-	Organisation must assure that data are fit for purpose and should prevent misuse;	Data accurate and complete, relevant and timely for the purpose (P3);	accurate, relevant, up to date (Article 5d);	Accurate, complete and kept up-to-date (s 8);
Informing individuals						
8	Notice	"There should be arrangements whether individual should know" (para.595);	Information about data uses (P4, p.62); Notification about data use before they can be used (P5, p.63);	Full knowledge – what data, why, how they will be used, by whom, for what purpose, how long (P1);	About the existence of 'file' (Article 8a), and about the fact that one's data are there (Article 8b);	Confirmation that controller has data (s 13a); Knowledge or consent, only where appropriate (s 7);
9	Openness / transparency principle	-	No secret registries (P1, p.59), Added as a principle by the US Privacy Act 1974;	Supplementary – as a means to an end (para.21.10);	-	General policy of openness about developments, practices, and policies (s 12);
Participation / Controlling						
10	Choice / consent / aka 'collection limitation'	-	-	Use only for the purposes made known or authorised (P6);	-	Knowledge *or* consent, only where appropriate (s 7);
11	Purpose specification / use limitation	Information held for purpose and not used for other purposes without appropriate authorisation (para.592);	Way to prevent of reuse for other purposes without consent (P3, p.61) limits on use, collection, and disclosure added as a	Only to the extent and for the purposes made known when they are obtained, or subsequently authorised (P2);	Data only to be used in specified purposes as a part of quality criterion (Article 5b), also sensitive data should not be	Purpose specification (s 9) – data use limited to fulfilment of purposes specified at collection or others not incompatible

			principle by the US Privacy Act 1974;		processed without appropriate safeguards;	and specified on each change of purpose use limitation (s 10) Other purposes only with the consent or by the authority of the law;
12	Access	"Right to printout" – enabling individuals to know what is recorded about them and to whom it was supplied (para.618);	Way to find out what is kept and how it is used (P2, p.59);	Not specified as regarded as a means to an end (para.21.10);	Confirmation of data processing as well as communication to him of such data (Article 8b);	Individual participation principle (s 13b) – right to have data communicated;
13	Correction	Accuracy, existence of correction and update mechanism (para.599);	Right to contest data, correct on request, on disagreement individual's claim appended (P6, p.63);	-	Rectification or erasure if not lawful and fair (Article 8c);	Individual participation principle (s 13d) – right to 'challenge' data;

B Comparison of Privacy Laws in the Researched Jurisdictions

Table 7 Privacy principles and rules in the selected jurisdictions

	Principles / laws	**Data Protection Directive (1995)** (Articles)	**NZ Privacy Act 1993** (principles)	**AUS Privacy Act 1988 (Cth)** (principles)	**CAN PIPEDA (2000)** (principles)	**General Data Protection Regulation (2016)** (Articles)
0	What value is balanced with privacy?	Free movement of personal data;	Not given. Privacy protection is shaped with 'general accordance with OECD guidelines';	Interests of entities in carrying out their functions or activities;	Electronic commerce;	Free movement of personal data;
General prerequisites						
1	Fairness and lawfulness	Article 6(1)(a) as a principle; Article 7 – six possible legal bases;	P4 – collected by not unlawful and not unfair means;	P3 – collection by lawful and fair means;	P4 – collection by fair and lawful means;	Article 5(1)(a) as a principle; Article 6(1) – 6 possible legal basis;
2	Data Protection Officer	-	Section 23;	-	P1 – individual accountable;	Article 37 – shall be appointed when processing has a large scale;
3	Accountability	Articles 22, 23 – judicial remedy, liability; Article 24 – administrative measures for Member States to decide;	Section 67 – first proceedings before Privacy Commissioner; Section 84 – remedy in proceedings before Human Rights Review Tribunal;	Section 52 – first complaint to Commissioner; determination not binding; Section 55A – proceedings in court to enforce; Section 80W – Commissioner may apply to court for civil	P1 – principle; P10 – internal procedure; Section 11 – first complaint with the Commissioner; Section 14 – hearing by Court with an option to award remedies (s 16);	Article 5(2) – principle; Article 24 – responsibility of controller; Article 28 – responsibility of processor; Article 79 – judicial remedy without DPA proceeding, before the

				penalties for serious, repetitive breaches;		court of data subject residence; Article 82 – right to compensation and liability; Article 83 – administrative fines;
Risk minimisation and quality						
4	Security	Article 16 – confidentiality Article 17 – obligation to implement measures of security;	P5 – protection;	P11 – protection;	P7 – safeguards;	Article 5(1)(f) – integrity and confidentiality principle; Article 32 – obligation to implement measures of security; Article 33 – notification about data breach to DPA;
5	Data minimisation	Article 6(c) 'not excessive';	P1 – collection limit to information necessary for the purpose; P9 – no longer than necessary;	P3 – collecting only data 'reasonably necessary';	P4 – limiting collection to what is necessary for the purpose; Section 5(3) – reasonableness test;	Article 5(1)(c) as a principle of storage limitation – 'limited to what is necessary'; Article 25 – Data Protection by design and default;
6	Separating identities from data	Article 6(e) as a principle; anonymisation when there is no other use for data (even extended);	P12 – unique identifiers not used if unnecessary;	P11 – deletion or anonymisation when no longer needed; P2 – anonymity and pseudonymity as an option for individual to contact organisations;	P5 – deletion or anonymisation when no longer necessary;	Article 5(1)(e) as a principle anonymisation as soon as possible; Pseudonymisation – as element of lowering the risk Articles 6(4),

						25, and security Article 32;
7	Quality	Article 6(d) – accurate, up to date;	P8 – accuracy;	P10 – accurate, up-to-date and complete; P3 – collection from individual;	P6 – accurate, complete and up-to-date;	Article 5(1)(d) – accuracy (accurate, up to date);
Informing individuals						
8	Notice / information	Articles 10, 11 – initial information about collection;	P2 – collection from data subject if possible; P3 – should be aware if possible;	P5 – notice; Section 26WL – notification about 'eligible data breach';	P3 – knowledge required to consent; Notification about breaches 'posing a real risk of significant harm';*	Articles 13, 14 – extensive initial information; Article 34 – notification about data breach;
9	Transparency / openness	– (mentioned in recitals);		P1 – open and transparent management of personal information;	P8 – openness of policies and practices;	Article 5(1)(a) as a principle; Article 12 – necessary in communication between parties;
Controlling						
10	Choice / consent	Articles 7(a), 8(2)(a) – one of the legal basis for data protection; Needed for changing purposes, or extending scope of processing; Article 14 – right to object in some cases when processing is not based on consent and	Not used as authorisation of data processing; But: P10 – may authorise new purpose; P11 – may authorise a disclosure;	Not used as authorisation of data processing; But: P6 – may authorise new purpose; P7 – may authorise use for direct marketing;	P3 – separate principle (!), rule that consent must be present; May be withdrawn subject to legal and contractual restrictions; But, s 7 – list of exceptions when consent not needed;	Articles 6(1)(a), 9(2)(a) – one of the legal basis for data protection; Needed for changing purposes, or extending scope of processing; Articles 7, 8 – conditions of validity, withdrawal;

		for the purpose of direct marketing;			P2 – may authorise new use;	Article 21 – right to object in some cases when processing is not based on consent and for the purpose of direct marketing;
11	Purpose specification / use limitation	Article 6(b) – purpose limitation;	P1 – purpose specification; P10 – purpose limitation. But, 'directly related' purposes allowed, also, other exceptions; P11 – disclosure limitation, but a number of exceptions;	P6 – purpose limitation, but also a number of exceptions;	P5 – limiting use, disclosure for purpose specified; But, exceptions in Sections 7(4) and 7(5);	Article 5(1)(b) – purpose limitation; Article 6(4) – changing purposes;
12	Access	Article 12(a) – right to access;	P6 – access; s11 - the only principle being a legal right;	P12 – access, but a number of exceptions;	P9;	Article 15 – right to access;
13	Correction	Article 12(b) – rectification;	P7;	P13;	P9 – when in accuracy was demonstrated;	Article 16 – right to rectification;
14	Erasure	Article 12(b) – erasure, claimed together with the right to object in *Google Spain*;	–	–	–	Article 17 – right to erasure, extension of the 'right to be forgotten' defined by ECJ;
15	Restriction of processing	Article 12(b) – narrow right to block data;	–	–	–	Article 18 – temporary restriction in case of dispute about data;
16	Data portability	–	–	–	–	Article 20 – right to take data, and right to

						have data transmitted to another service provider;
17	Automated individual decision making	Article 15 – limited right to not be subject of profiling decision basing solely on automated decision making;	–	–	–	Article 22 – broader right to not be subject of decision basing solely on automated decision making;

* - breach reporting introduced by the Canadian Digital Privacy Act, S.C. 2015, c. 25 will be specified in the secondary regulation.